Aportación Conjunta de Organizaciones de la Sociedad Civil y Academia sobre la X Cumbre de las Américas: “Construyendo un Hemisferio Seguro, Sostenible y de Prosperidad Compartida”

I. Introducción

Las organizaciones firmantes presentan en esta oportunidad insumos al proceso hacia la Décima Cumbre de las Américas, a realizarse en diciembre del 2025 en la República Dominicana. Esta aportación conjunta refleja un conjunto de preocupaciones relacionadas con la intersección entre tecnología y derechos humanos, y está dirigida a los Estados de las Américas que forman parte de la Cumbre.

La Décima Cumbre tiene el objetivo de reunir a los distintos países de la región para acordar compromisos y acciones que posicionen a las Américas como un hemisferio seguro, sostenible y de prosperidad compartida. El documento conceptual tiene como punto de partida la garantía de la seguridad humana en múltiples dimensiones, profundizando en cuatro ejes temáticos principales: seguridad ciudadana, seguridad alimentaria, seguridad energética y seguridad hídrica. Aunque no se mencione a las tecnologías digitales más directamente, las potencialidades y retos relativos a su desarrollo y utilización son parte de las políticas y acciones estatales y, por lo tanto, transversales a lo que plantea el documento conceptual.

Nuestra aportación se propone a abordar algunos de los aspectos más relevantes en este sentido, en aras de subrayar puntos clave que merecen la atención de los Estados, y ofrecer recomendaciones relevantes y concretas.

Esperamos que estos aspectos puedan ser considerados en el proceso de la Décima Cumbre y agradecemos por la oportunidad de escucha y participación.

II. Aspectos de tecnología relacionados al documento conceptual

1. Fortalecimiento del espacio cívico digital: infraestructura y conectividad, inclusión digital, participación ciudadana y transparencia

a. Contexto y retos

El espacio cívico digital se ha convertido en una dimensión esencial para el ejercicio de derechos, la participación ciudadana y la construcción democrática. Sin embargo, en muchos países de la región persisten retos estructurales que limitan el acceso significativo a las tecnologías digitales. Entre ellos, se destacan la brecha de infraestructura, la desigualdad en la conectividad, la falta de políticas inclusivas y la escasa transparencia en el uso estatal de tecnologías. Estos desafíos impiden que amplios sectores de la población ejerzan plenamente sus derechos en entornos digitales.

La seguridad humana, que busca la dignidad y el bienestar de cada individuo, y la seguridad ciudadana, centrada en la convivencia pacífica, son inseparables del espacio cívico digital en el siglo XXI. Sin embargo, este espacio no puede desarrollarse sin una base sólida de infraestructura digital y conectividad significativa, una verdadera inclusión digital y la participación ciudadana y transparencia en la formulación de políticas públicas. Estos tres elementos son interdependientes y cruciales para construir sociedades más seguras y resilientes.

b. Infraestructura y conectividad

Una infraestructura digital robusta y una conectividad universal y significativa son precondiciones para el desarrollo socioeconómico de nuestras sociedades.[1] Sin ellas, amplias franjas de la población quedan excluidas de información y oportunidades vitales (ej. educación, empleo, cultura), servicios esenciales y canales de participación ciudadana. Esto genera condiciones con impacto negativo en la seguridad ciudadana.

De ahí la importancia de tomar pasos activos para reducir las distintas y persistentes brechas

[1] La conectividad universal y significativa es el acceso a internet que va más allá de la mera disponibilidad, asegurando que la experiencia en línea sea segura, satisfactoria, enriquecedora y productiva a un costo asequible. Implica no solo que las personas puedan conectarse, sino que lo hagan de una manera —con dispositivos adecuados, habilidades digitales, y un uso que genere valor social real— que les permita aprovechar plenamente las oportunidades digitales para mejorar sus vidas.
Vease A4AI (2022). *Advancing Meaningful Connectivity: Towards Active & Participatory Digital Societies*.
Disponible en https://a4ai.org/report/advancing-meaningful-connectivity-towards-active-and-participatory-digital-societie s/, y NIC.br. (2024). Conectividad significativa: propuesta de medición y el retrato de la población en Brasil. *Cuandernos NIC.br Estudios Sectoriales*. Disponible en https://cetic.br/media/docs/publicacoes/7/20240606120955/estudios_sectoriales_conectividad

digitales,[2] mejorando el acceso y la asequibilidad a Internet, facilitando el conocimiento y el contenido multilingüe y desarrollando habilidades digitales. Al garantizar que las personas tengan acceso universal y significativo a la red, se habilita el acceso a la educación, la cultura, la salud, el empleo y la información, pilares clave para la seguridad humana.

RECOMENDACIONES

- Impulsar políticas que garanticen una Internet de banda ancha segura y asequible para todas las personas, reconociendo el acceso a la red como un derecho esencial para la participación plena en la sociedad y la economía digital. Esto incluye la diversificación del acceso a través de esfuerzos impulsados localmente (ej. redes comunitarias), formas innovadoras de financiar la conectividad (ej. mecanismos de financiación mixta), y el impulso hacia un auténtico multilingüismo en Internet.
- Promover la interoperabilidad para evitar la dependencia de proveedores privados, haciendo la conectividad más resiliente y accesible. Esto incluye prestar mayor atención a soluciones tecnológicas de código abierto (*open-source*). Estas pueden ayudar a reducir costos y permitir a las comunidades auditar y adaptar la tecnología a sus necesidades, fomentando la innovación local y la transparencia en la gestión de redes.
- Asegurar que las políticas de conectividad cuenten con mecanismos de supervisión y evaluación periódica, mediante procesos participativos que incluyan a las comunidades, organizaciones de la sociedad civil y actores técnicos. Estos mecanismos deben garantizar transparencia, rendición de cuentas e incorporación de aprendizajes para su mejora continua.

c. Inclusión digital

La inclusión digital implica que cada persona posea las habilidades y el conocimiento para usar y apropiarse de la tecnología de forma segura, crítica y productiva según sus intereses personales y los de sus comunidades. Al dotar a las personas de habilidades digitales, se fortalecen sus capacidades para la autoprotección, el desarrollo personal y la participación informada en la vida pública, mejorando su bienestar general y el de la sociedad.[3]

Sin embargo, es crucial reconocer que la brecha digital de género es un obstáculo significativo para esta inclusión plena. No solo limita la participación de las personas por motivos de género en el entorno digital, sino que las hace más vulnerables a las violencias facilitadas por la tecnología (ej. ciberacoso, difusión no consentida de contenido íntimo, etc.) y a las múltiples exclusiones derivadas de la brecha digital, en un contexto de transformación digital y digitalización de múltiples servicios públicos.[4] Las desigualdades de género existentes en el

[2] A pesar de los avances, aún persisten brechas digitales entre distintos grupos de ingresos, grupos etarios, zonas geográficas y grupos de género.
[3] *Véase* Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. (2024). Acceso universal a internet y alfabetización digital. *Inclusión digital y gobernanza de contenidos en internet*. OEA/Ser.L/V/II.
[4] CEPAL. (2023). Erosionar los nudos estructurales de la desigualdad de género: la violencia contra las mujeres y las niñas como un problem crítico en la era digital. Disponible en https://repositorio.cepal.org/server/api/core/bitstreams/004a1622-6809-41c4-ab52-c83b8a6fbd81/content

mundo fuera de línea se replican y amplifican en los entornos en línea, por lo que urgen programas de inclusión digital con perspectiva de género.

Todos los elementos mencionados no operan en silos. Una mejor infraestructura permite mayor conectividad, lo que facilita la inclusión digital. Entornos digitales más inclusivos permiten que un mayor número de personas participen de los procesos de formulación de políticas públicas. Esta participación requiere y fomenta la transparencia, que a su vez construye confianza y fortalece la seguridad ciudadana. Para ello, se necesitan protecciones para las personas que están ejerciendo sus derechos participando en la vida pública. Juntos, estos pilares construyen un espacio cívico digital que no solo es un reflejo de democracias sólidas, sino una herramienta indispensable para alcanzar una seguridad humana y ciudadana integral y duradera en la región.

RECOMENDACIÓN

- Implementar programas de alfabetización informacional y mediática para todas las edades, con un énfasis especial en el pensamiento crítico. El objetivo es que las personas no solo sepan usar la tecnología, sino que comprendan sus derechos en línea y tomen decisiones informadas para protegerse a sí mismas y a sus comunidades, fortaleciendo así el tejido social.

2. Seguridad ciudadana y tecnologías de vigilancia

a. Contexto y retos

Durante la última década, los Estados de la región han incrementado sus capacidades de vigilancia sobre la base de garantizar la seguridad de la población, lo que se ha expresado en la adopción creciente de tecnologías y prácticas cada vez más intrusivas, a menudo, sin la debida transparencia ni marcos regulatorios que garanticen una adecuada supervisión ni rendición de cuentas.[5]

La falta de garantías en la aplicación de este tipo de medidas supone un riesgo para el pleno goce de los derechos humanos. Particularmente, el derecho a la privacidad, que se considera un habilitador del ejercicio de otros derechos fundamentales[6] y guarda un nexo estrecho con la libertad de expresión,[7] que solo puede ejercerse plenamente cuando existe una “esfera privada,

[5] Oficina del Alto Comisionado de ONU para los Derechos Humanos – México. Declaración de la Alta Comisionada de la ONU para los Derechos Humanos, Michelle Bachelet, sobre el uso de software espía para vigilar periodistas y personas defensoras de derechos humanos, julio de 2021. https://hchr.org.mx/comunicados/declaracion-de-la-alta-comisionada-de-la-onu-para-los-derechos-human os-michelle-bachelet-sobre-el-uso-de-software-espia-para-vigilar-periodistas-y-personas-defensor as-de-d erechos-humanos/

[6] Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/29/32), mayo de 2015. https://documents.un.org/doc/undoc/gen/g15/095/85/pdf/g1509585.pdf [7] Centro de Estudios en Libertad de Expresión (CELE), Contribution to the preparation of the report on the challenges and risks regarding discrimination and the unequal enjoyment of the right to privacy associated with the collection and processing of data, mayo de 2025. https://www.palermo.edu/Archivos_content/2025/cele/mayo/dp27.pdf

libre de la injerencia arbitraria del Estado".[8] A su vez, la persecución de discursos críticos muchas veces tiene como consecuencia la implementación de medidas que erosionan el derecho a la privacidad.

La televigilancia de espacios públicos y la incorporación de tecnologías de identificación biométrica, la Inteligencia de Fuentes Abiertas (OSINT),[9] la adquisición y uso de software espía, la interceptación de comunicaciones, y otras formas de control utilizadas para monitorear, intimidar o silenciar periodistas, defensores de derechos humanos y otras formas de disidencia, viola la privacidad, desalientan el libre intercambio de ideas y debilitan la participación democrática, como ha señalado la Relatoría Especial para la Libertad de Expresión (RELE) de la Organización de los Estados Americanos (CIDH).[10]

Estas prácticas, cuando no están debidamente reguladas ni supervisadas, pueden constituir violaciones directas a los estándares del Sistema Interamericano de Derechos Humanos. La Corte Interamericana ha afirmado que la vigilancia encubierta, la interceptación de comunicaciones o la recopilación masiva de datos personales constituyen injerencias graves a los derechos fundamentales protegidos por la Convención Americana sobre Derechos Humanos. Estas medidas deben cumplir estrictamente con el principio de legalidad, perseguir fines legítimos, ser necesarias y proporcionales, y contar con salvaguardas efectivas, como autorización judicial previa, control institucional independiente y recursos judiciales efectivos.[11]

El caso *Miembros de la Asociación Civil de Derechos Humanos (CAJAR) vs. Colombia* constituye un precedente fundamental en la región: la Corte Interamericana estableció que los Estados deben prevenir la vigilancia ilegal y asegurar la protección de datos personales, garantizando la autodeterminación informativa, el acceso a la información y mecanismos efectivos de supervisión y rendición de cuentas.[12]

El proceso de la Cumbre debe tener especialmente en cuenta el desarrollo de estándares y garantías en el marco del Sistema Interamericano de Derechos Humanos. La Comisión Interamericana ha subrayado que la seguridad ciudadana se concibe como una política

---

[8] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression. *Freedom of expression and the Internet.* Diciembre de 2013, para. 130. https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_Internet_ENG%20_WEB.pdf

[9] Nicolás Zara, Inteligencia basada en fuentes abiertas (OSINT) y derechos humanos en Latinoamérica: un estudio comparativo en Argentina, Brasil, Colombia, México y Uruguay (CELE), 2023, p. 45.

[10] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression. *Inclusión digital y gobernanza de contenidos en internet.* Junio de 2024, para. 62. https://www.oas.org/es/cidh/expresion/informes/Inclusion_digital_esp.pdf

[11] Caso Miembros de la Corporación Colectivo de Abogados "José Alvear Restrepo" (CAJAR) vs. Colombia, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 18 de octubre de 2023. https://jurisprudencia.corteidh.or.cr/es/vid/953775991., para. 547, 551, 553 y 562. La decisión del juez debe basarse en los criterios para la restricción o limitación admisible del derecho a la vida privada y libertad de expresión, conocido como test tripartito (ver para. 521).

[12] Id. Estos controles incluyen la supervisión de los servicios de inteligencia por una institución civil independiente y la posibilidad de reclamo frente a actuaciones arbitrarias (ver para. 564-565). Incluyen también el debido registro de las actividades de inteligencia emprendidas en todas sus etapas (ver para. 540).

pública.[13] En este sentido, el diseño, implementación y evaluación de políticas de seguridad ciudadana deben regirse por los principios internacionales de derechos humanos, "especialmente, los principios de participación, rendición de cuentas, y no-discriminación".[14] La Comisión ha señalado la carencia de mecanismos efectivos de rendición de cuentas, que aseguren una gestión transparente y favorezcan distintas modalidades de control por parte de la ciudadanía, como una de las mayores trabas para el debido cumplimiento de los Estados a los derechos comprometidos en materia de seguridad ciudadana.[15]

En este marco, la autorización judicial previa, debidamente motivada, es fundamental para llevar a cabo distintas acciones de vigilancia amparadas en tecnologías digitales. La autodeterminación informativa también está garantizada por la Convención Americana de Derechos Humanos[16] y debe asegurarse en el contexto de la vigilancia estatal. Las restricciones a este derecho deben ser estrechamente concebidas, debidamente fundamentadas y limitadas en el tiempo.

RECOMENDACIONES

- Como ha señalado la Asamblea General y el Consejo de Derechos Humanos de la Organización de Naciones Unidas, los Estados deben abstenerse de realizar prácticas de vigilancia ilegal y arbitraria, y tienen la obligación de garantizar el ejercicio del derecho a la libertad de expresión.[17]

- Fortalecer la seguridad ciudadana en el entorno digital mediante el uso y cumplimiento proporcional de marcos legales precisos, evitando el uso concentrado y centralizado del derecho penal como instrumento para afrontar todas las posibles amenazas que puedan vulnerar la seguridad en línea. Las medidas que se adopten para lograr este objetivo deberán cumplir con el test tripartito de legalidad, necesidad y proporcionalidad del Sistema Interamericano de Derechos Humanos.

- Abstenerse de desarrollar, adquirir o desplegar tecnologías de vigilancia y sistemas automatizados que no garanticen el pleno respeto a los derechos humanos, conforme a los estándares internacionales de derechos humanos. Esto incluye considerar medidas como moratorias o prohibiciones cuando las tecnologías impliquen riesgos sustanciales y no mitigables para los derechos fundamentales, en línea con lo señalado por la Asamblea General de las Naciones Unidas.[18]

---

[13] CIDH, Informe sobre Seguridad Ciudadana y Derechos Humanos, 31 de diciembre de 2009, para. 52. https://www.oas.org/es/cidh/docs/pdfs/seguridad%20ciudadana%202009%20esp.pdf
[14] Id., para. 51.
[15] Id., para. 95.
[16] Refiere al derecho a acceder y controlar sus datos personales, incluyendo las facultades del titular de datos de obtener más informaciones sobre qué datos relativos a él se encuentran en los registros de los órganos públicos, reclamar su rectificación o modificación, exigir su eliminación en casos determinados, entre otros. Id., para. 570 y 582-588.
[17] Inter-American Commission on Human Rights. Office of the Special Rapporteur for Freedom of Expression.
Freedom of expression and the Internet. December 31 2013, para. 23. https://www.oas.org/en/iachr/expression/docs/reports/2014_04_08_internet_eng%20_web.pd

- Asegurar que toda política pública de seguridad ciudadana, así como las actividades de inteligencia o persecución penal, se desarrollen en cumplimiento de los principios de participación, rendición de cuentas y no discriminación. Los Estados deben contar con estructuras institucionales y recursos que garanticen una gestión democrática y basada en derechos, incluyendo mecanismos de supervisión independientes con facultades y autonomía técnica.
- Incorporar salvaguardas como la autorización judicial previa debidamente motivada, la existencia de mecanismos de remedio efectivo y el respeto a la protección de datos y a la autodeterminación informativa también en las actividades de seguridad pública, tal como garantiza la Convención Americana de Derechos Humanos.

b. Participación ciudadana y transparencia

La participación activa de la ciudadanía en la formulación y seguimiento de las políticas públicas de seguridad, incluyendo las que involucran tecnologías digitales, las hace más legítimas, pertinentes y efectivas.[19] Cuando las soluciones nacen del diálogo con la comunidad, se reduce la desconfianza en las instituciones y se asegura que las políticas aborden las preocupaciones reales de las comunidades y las personas.

La transparencia es esencial para salvaguardar la privacidad y la libertad de expresión, que son derechos fundamentales para la seguridad humana. Es crucial que la adquisición, despliegue y uso de tecnología por parte de los gobiernos para propósitos de seguridad —como las herramientas de vigilancia— sea transparente y basada en derechos humanos. Su ausencia genera desconfianza y temor a la arbitrariedad o al abuso de poder. Cuando hay transparencia, las personas y comunidades pueden fiscalizar y exigir rendición de cuentas, fortaleciendo así el estado de derecho y las libertades individuales.

RECOMENDACIONES

- Diseñar estrategias y mecanismos accesibles y transparentes para la consulta pública, la presentación de propuestas y el monitoreo ciudadano de políticas públicas de seguridad, incluyendo las que involucren la implementación de capacidades tecnológicas del Estado. La transparencia sobre la adquisición, despliegue y uso de tecnologías por parte del Estado debe ser la norma, no la excepción.
- Crear y/o fortalecer entes de supervisión independientes, con facultades robustas y estructuras compatibles con sus competencias, que garanticen la fiscalización efectiva, el cumplimiento del derecho de acceso a la información y que cuenten con mecanismos de rendición de cuentas ante la ciudadanía.

---

[18] United Nations General Assembly. *Resolution A/RES/78/265*. Marzo de 2024. https://docs.un.org/en/A/RES/78/265

[19] Open Government Partnership. (s.f.). *Integración de la participación*. Disponible en https://www.opengovpartnership.org/es/open-gov-guide/open-government-foundations-mainstreaming-par ticipation/.

3. Digitalización del Estado e innovación ancladas en derechos humanos

a. Contexto y retos

En los últimos años, los Estados de América Latina han acelerado significativamente la digitalización de la gestión pública. Este proceso ha sido impulsado principalmente por una apuesta por incrementar la eficiencia y modernizar los trámites y servicios públicos, así como en aumentar su transparencia. En efecto, la IX Cumbre de las Américas, realizada en 2022, ha adoptado compromisos en esta dirección, en el marco de un Programa Regional para la Transformación Digital.[20]

Sin embargo, investigaciones recientes han identificado que sistemas total o parcialmente automatizados y tecnologías basadas en inteligencia artificial (IA) han sido implementadas en sectores clave de la administración pública sin diagnósticos adecuados que las avalen, ni mecanismos de evaluación periódicos.[21] En muchos casos, tampoco han sido observados los compromisos de legalidad, necesidad y proporcionalidad previstos en los estándares internacionales de derechos humanos y reforzados por el Consejo de Derechos Humanos de la ONU.[22]

La velocidad del despliegue tecnológico no ha sido acompañada por acciones de fortalecimiento de garantías y protecciones capaces de prevenir y responder a eventuales abusos. Por un lado, aún existen países con marcos normativos desactualizados o insuficientes en materia de transparencia pública y protección de datos; por otro, las reglas existentes muchas veces no son observadas adecuadamente. Este escenario ha permitido el desarrollo de iniciativas que afectan derechos fundamentales de la población, especialmente de los sectores en condiciones más vulnerables.

---

[20] Mandatos adoptados en la IX Cumbre de las Américas, Programa Regional para la Transformación Digital. Disponible en: https://www.summit-americas.org/Publications/IX_Summit/Mandatos%20adoptados%20IX%20Cumbre% 20ESP%20DIGITAL.pdf.

[21] García, J. M. Inteligencia Artificial en el Estado: Estudio colectivo sobre experiencias y riesgos para los derechos humanos. Derechos Digitales, 2024. Disponible en: https://ia.derechosdigitales.org/wp-content/uploads/2025/02/2024-LATAM-IA_en_el-Estado-EN.pdf y Velasco, P. & Venturini, J. Decisiones automatizadas en la función pública en América Latina. Derechos Digitales, 2021. Disponible en: https://ia.derechosdigitales.org/wp-content/uploads/2021/03/CPC_informeComparado.pdf.

[22] Consejo de Derechos Humanos. A/HRC/48/31. El derecho a la privacidad en la era digital. 2021. Disponible en: https://docs.un.org/es/A/HRC/48/31.

Sistemas como el SINE en Brasil[23], Alerta Niñez en Chile[24] y PretorIA en Colombia[25] ilustran esta problemática. Estos sistemas han sido usados para priorizar intervenciones sociales, detectar "riesgos" en familias o incluso para apoyar decisiones judiciales, sin mecanismos efectivos de control o rendición de cuentas. Es decir, estas tecnologías determinan el acceso a políticas públicas o servicios sociales sin que existan mecanismos claros de verificación democrática o posibilidad de apelación por parte de quienes son afectados.

Este avance tecnológico ocurre en un contexto regional de alta desigualdad, con baja participación de los países latinoamericanos en el diseño de estas tecnologías, así como de fuerte dependencia tecnológica.[26] En muchos casos, los Estados adoptan sistemas que no controlan ni entienden plenamente, aumentando su vulnerabilidad institucional y debilitando la soberanía tecnológica de la región.[27] Además, las decisiones se toman sin mecanismos de consulta o diálogo público, lo que agrava los riesgos de exclusión, discriminación y abusos.

Esto adquiere aún más relevancia ante el riesgo de que las inversiones en digitalización e inteligencia artificial desvíen recursos esenciales destinados a programas sociales fundamentales, especialmente en contextos de ajustes fiscales o recortes presupuestarios, como lo ha advertido la Relatoría Especial sobre el derecho a la salud de Naciones Unidas.[28]

RECOMENDACIÓN

- Adoptar marcos normativos que aseguren que todo proceso de digitalización del Estado esté basado en principios de derechos humanos, aplicando los criterios de legalidad, necesidad y proporcionalidad desde su diseño.[29]

---

[23] Bruno, F.; Cardoso, P.; Faltay, P. Sistema Nacional de Empleo y la gestión automatizada de la desocupación laboral. Derechos Digitales, 2021. Disponible en: https://ia.derechosdigitales.org/wp-content/uploads/2022/03/03_Informe-Brasil-EN_180222_compressed. pdf

[24] Valderrama, M. Sistema Alerta Niñez y la predicción del riesgo de vulneración de derechos de la infancia. Derechos Digitales, 2021. Disponible en https://ia.derechosdigitales.org/wp-content/uploads/2021/03/CPC_informe_Chile.pdf.

[25] Saavedra, V.; Upegui, J. C. PretorIA y la automación del procesamiento de causas de derechos humanos. Derechos Digitales, 2021. Disponible en https://ia.derechosdigitales.org/wp-content/uploads/2021/03/CPC_informe_Colombia.pdf.

[26] Matías González Mama, Agustín Pérez Aledda, y Lina Palacios, "Gobernanza global de la IA: ¿quién regula, con qué enfoque y para quién?", Artículo de investigación No. 67 (ESP), Centro de Estudios en Libertad de Expresión (CELE), Buenos Aires (2025), p. 46 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5311517

[27] Derechos Digitales. Inteligencia Artificial, derechos humanos y justicia social. Derechos Digitales, 2024. Disponible en: https://ia.derechosdigitales.org/wp-content/uploads/2025/03/DD_GIRAI_ESP_2024.pdf.

[28] Consejo de Derechos Humanos. A/HRC/53/65. Innovación digital, tecnologías y derecho a la salud. Disponible en: https://docs.un.org/es/A/HRC/53/65.

[29] La aplicación de estándares interamericanos de derechos humanos también juega un rol esencial. En este sentido, ver Alimonti, A.; Alcântara, R. C. Estándares interamericanos y uso estatal de la IA en decisiones que afecten derechos humanos: implicaciones para los DDHH y marco operativo. Electronic Frontier Foundation, 2024. Disponible enhttps://www.eff.org/document/estandares-de-derechos-humanos-para-el-uso-estatal-de-la-ia-en-americ a-latina

b. Participación y transparencia

La adopción de sistemas digitales y/o automatizados en el sector público no ha sido precedida o acompañada de espacios para la participación ciudadana. No existen marcos institucionales que garanticen una participación efectiva y sostenida de la sociedad civil en las decisiones tecnológicas del sector público. A su vez, las iniciativas voluntarias de consultas públicas en procesos decisorios relacionados se mostraron insuficientes para garantizar una participación significativa, en particular para las personas potencialmente más afectadas.[30]

Tampoco se han establecido espacios de consulta estructurados ni procesos de evaluación pública de las herramientas utilizadas.[31] Las políticas digitales suelen definirse desde organismos centrales, sin diálogo previo con actores sociales ni con los sectores encargados de su implementación en los territorios.[32]

La transparencia es otro punto crítico. Muchas de las decisiones sobre tecnologías en el sector público —incluyendo convenios con empresas proveedoras, selección de plataformas o diseño de algoritmos— se toman sin información accesible. Los contratos rara vez incluyen obligaciones de divulgación, auditoría externa o publicación del código fuente; tampoco involucran tecnologías de código abierto, lo que impide el control ciudadano.[33]

Cuando se trata de acceso a la información, aún cuando existen normativas sobre el tema, se observan barreras que incluyen la falta de respuesta sobre cuestiones críticas relacionadas a los sistemas y tecnologías adoptados, respuestas incompletas a solicitudes de información, negativa en brindar respuestas o entrega de datos desactualizados, alegaciones de secreto y ausencia de medidas pro-activas de transparencia. Además, no se han desarrollado estándares comunes para garantizar que la información sobre sistemas automatizados sea comprensible y relevante para las personas afectadas. En ausencia de transparencia técnica y administrativa, la digitalización del Estado se vuelve un proceso opaco, difícil de fiscalizar y alejado de los principios democráticos.

---

[30] García, J. M.; Venturini, J. Participação Cidadã e Regulação da Inteligência Artificial: Análise da Composição Setorial das Audiências Públicas na CJSUBIA. Revista Internet & Sociedade. Vol. 5, n. 1., 2024. Disponible en: https://revista.internetlab.org.br/participacao-cidada-e-regulacao-da-inteligencia-artificial-analise-da-comp osicao-setorial-das-audiencias-publicas-na-cjsubia/ y Hernández, L.; Canales, M. P.; Souza, M. Inteligencia artificial y participación en América Latina: Las estrategias nacionales de IA. Derechos Digitales, 2022. Disponible en: https://ia.derechosdigitales.org/wp-content/uploads/2022/06/IA-Participacion-ES-2022.pdf.

[31] Velasco, P. & Venturini, J. Decisiones automatizadas en la función pública en América Latina. Derechos Digitales, 2021. Disponible en: https://ia.derechosdigitales.org/wp-content/uploads/2021/03/CPC_informeComparado.pdf.

[32] Mantilla-León, L. C.; Camacho, L. Aprendizajes de la gobernanza de internet para la gobernanza de IA: un enfoque de participación significativa desde América Latina. Derechos Digitales, 2024. Disponible en: https://ia.derechosdigitales.org/wp-content/uploads/2025/03/Participacio%CC%81n-significativa_2024_E S.pdf.

[33] Ibidem.

RECOMENDACIONES

- Garantizar la participación significativa de la sociedad civil en la toma de decisiones y monitoreo a la implementación de tecnologías en los servicios públicos, incluyendo mecanismos accesibles y representativos para pueblos indígenas, comunidades rurales, mujeres, personas con discapacidad, juventudes y otros sectores históricamente marginalizados, respetando su derecho a la consulta previa cuando corresponda.
- Exigir evaluaciones de impacto en derechos humanos previas a la implementación de sistemas de decisión automatizada en el sector público. Estas evaluaciones deben ser significativamente participativas, interdisciplinarias y de acceso público, de acuerdo
  con la Recomendación de la Unesco sobre la ética de la inteligencia artificial.[34]
- Incluir cláusulas de transparencia, auditoría independiente y acceso al código fuente o sus equivalentes en toda contratación de soluciones tecnológicas por parte del Estado.
- Promover el desarrollo de soluciones de tecnología de código abierto (*open-source*) para aumentar la transparencia y permitir que la sociedad civil y las personas auditen y entiendan cómo funcionan estas herramientas, impulsando habilidades para cuestionar el uso de la tecnología.
- Fortalecer las instituciones responsables de fiscalizar e implementar normativas de acceso a la información e implementar medidas de transparencia activa relacionadas a la adquisición y despliegue de tecnologías en el sector público, en particular para la entrega de servicios públicos esenciales.[35]

c. Protección de datos y ciberseguridad

Uno de los aspectos más críticos de la digitalización del Estado es el manejo de los datos personales. La creciente recolección y procesamiento de información sensible por parte de organismos públicos requiere normativas específicas que, en la mayoría de los países de América Latina, aún son inexistentes o insuficientes. Incluso donde existen marcos legales, estos enfrentan una aplicación débil o ineficaz, lo que evidencia la necesidad no sólo de nuevas normas, sino del fortalecimiento de los mecanismos de cumplimiento y supervisión.

En muchos países de la región no existen leyes actualizadas de protección de datos o las que existen presentan vacíos importantes. Una de las principales debilidades es la existencia de excepciones amplias que permiten el uso de datos personales en el contexto de políticas públicas, incluso para fines distintos de aquellos para los que fueron recolectados. Esta práctica erosiona el principio de finalidad y expone a la población a un uso indebido de sus datos.

A esto se suma la falta de independencia de las entidades responsables de supervisar el cumplimiento de normas sobre datos personales, cuando ellas existen. En varios casos, las agencias de control carecen de autonomía técnica, recursos o herramientas para actuar frente a abusos.

[34] UNESCO. Disponible en: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa.
[35] Véase también
https://www.eff.org/pages/recommendations-operational-framework?language=es#Transparency

En cuanto a la ciberseguridad, los diagnósticos regionales muestran que muchos países no cuentan con estrategias robustas ni con protocolos para responder a incidentes. Algunos aún carecen de planes nacionales en la materia.[36] Las filtraciones de bases de datos públicas, el acceso indebido a sistemas estatales y la comercialización ilegal de información ciudadana son problemas frecuentes.[37] Además, no existen protocolos claros para notificar a las personas afectadas por filtraciones de datos o accesos indebidos, lo que limita su capacidad de defensa y reparación.

En contextos de creciente digitalización, esta falta de respuesta institucional agrava la exposición de grupos en situación de riesgo. Las brechas de género también son una constante: las estrategias de protección digital rara vez contemplan medidas específicas para mujeres, personas LGBTQIA+ o comunidades que enfrentan mayores niveles de vigilancia o violencia estructural.[38]

RECOMENDACIONES

- Fortalecer la aplicación efectiva de las obligaciones legales ya existentes en materia de derechos humanos, protección de datos y ciberseguridad, incluyendo la creación o fortalecimiento de las instituciones de supervisión y fiscalización.
- Evitar el uso secundario de datos personales recolectados en servicios públicos para entrenar sistemas de inteligencia artificial sin consentimiento explícito, libre e informado, más allá al respeto a los principios de necesidad y proporcionalidad.

III. Recomendaciones a la cooperación regional

[36] Lara, J. C. Ciberseguridad en América Latina: estrategias nacionales en 2024. Derechos Digitales, 2025. Disponible en: https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ESP_2024.pdf [37] Son algunos ejemplos de la región: LA NACIÓN. Nueva filtración de Renaper: qué pasó esta vez con la publicación de datos de ciudadanos argentinos, y qué hay que hacer. 2024. Disponible en: https://www.lanacion.com.ar/tecnologia/nueva-filtracion-de-renaper-que-paso-esta-vez-con-la-publicacion -de-datos-de-ciudadanos-argentinos-y-nid09042024/; G1. Nova falha do Ministério da Saúde expõe dados de 243 milhões de brasileiros na internet, diz jornal. 2020. Disponible en: https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-d ados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml; MINISTERIO DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN DE PARAGUAY. MITIC informa sobre presunta filtración de datos sensibles. 2025. Disponible en: https://mitic.gov.py/mitic-informa-sobre-presunta-filtracion-de-datos-sensibles/.
[38] APC. A framework for developing gender-responsive cybersecurity policy norms, standards and guidelines. 2022. Disponible en: https://www.apc.org/en/pubs/framework-developing-gender-responsive-cybersecurity-policy-norms-stand ards-and-guidelines.

La cooperación regional en materia de derechos humanos y tecnologías es cada vez más relevante para enfrentar desafíos comunes y promover soluciones compartidas. En el marco del proceso de la Cumbre de las Américas, se identifican espacios clave donde los Estados pueden coordinar esfuerzos, alinear principios rectores y marcos normativos y fortalecer capacidades, con miras a garantizar que la transformación digital se base en los derechos humanos, la inclusión y la justicia social. Las siguientes recomendaciones apuntan a contribuir con ese objetivo.

1. Marcos normativos y cooperación institucional basada en derechos

- Asentar la creación de la Plataforma Hemisférica de Seguridad Ciudadana y Comunitaria en un mandato claro de respeto, promoción y protección de los Derechos Humanos. Esto implica que el intercambio de información y la coordinación de esfuerzos operen bajo estrictos principios de legalidad, necesidad, proporcionalidad y transparencia, con la implementación de sólidos mecanismos de supervisión y rendición de cuentas que salvaguarden eficazmente a las personas y que garanticen la participación de múltiples partes interesadas.
- Desarrollar e implementar estándares y mecanismos regionales de cooperación que rijan la gobernanza democrática de datos y el uso ético de tecnologías. Estos instrumentos deben asegurar que la recopilación, procesamiento y utilización de datos en la región se realicen bajo el respeto al derecho a la privacidad y a la no discriminación, de acuerdo a legislaciones robustas de protección de datos, con el cumplimiento de sus princípios generales, la garantía del consentimiento libre e informado y de los derechos ARCO[39], así como de una supervisión independiente efectiva.
- Establecer una moratoria temporal en las Américas sobre la inversión que realizan los bancos de desarrollo y mecanismos internacionales de financiación en la implantación de sistemas, prácticas y tecnologías digitales de vigilancia. La moratoria debe mantenerse hasta que se realice y publique una revisión exhaustiva de la evidencia existente. Tras dicha revisión, los marcos de contratación para futuras colaboraciones deben centrarse en asegurar el cumplimiento de las obligaciones en materia de Derechos Humanos, prestando especial atención a situaciones donde su protección sea deficiente o exista un mayor riesgo de exclusión.

2. Transparencia, evaluación y rendición de cuentas en el uso de tecnologías en la función pública

[39] Los derechos ARCO son una expresión de la autodeterminación informativa y se refieren a los derechos de acceso, rectificación, cancelación y oposición.

- Evaluar la evidencia existente en la región sobre el riesgo de violaciones de derechos humanos relacionadas con el despliegue de tecnologías con capacidades de vigilancia. Con base en esa evaluación, deben cesar las actividades que aumentan dicho riesgo. Es fundamental que el asesoramiento, los diagnósticos, las inversiones y el apoyo técnico interestatal y desde organismos internacionales cuenten con una sólida base empírica, en particular en lo que respecta al impacto de estas tecnologías en los derechos humanos, incorporando activamente las contribuciones de la sociedad civil, la academia y el sector tecnológico para enriquecer la evaluación desde perspectivas diversas y expertas.
- Intercambiar buenas prácticas sobre mecanismos de transparencia y rendición de cuentas en la adquisición, despliegue y uso de tecnologías de vigilancia, con el objetivo de garantizar el acceso a la información pública.
- Exigir una mayor transparencia en las actividades de las organizaciones internacionales y empresas de tecnología para la vigilancia. Esto implica la publicación de contratos con el poder público y de evaluaciones de impacto en Derechos Humanos según los Principios Rectores sobre las Empresas y Derechos Humanos de la ONU y auditorías técnicas, junto con la implementación de mecanismos de rendición de cuentas que permitan a la sociedad civil y otras partes interesadas acceder a información y exigir responsabilidades.También incluye establecer sanciones para asegurar que solo se implementen sistemas que respeten plenamente los Derechos Humanos.
- Aumentar la financiación y los recursos destinados a estudios de referencia, análisis contextuales regionales y de costo-beneficio, y a evaluaciones independientes basadas en derechos humanos. Esto incluye la asignación de fondos y recursos para llevar a cabo las evaluaciones basadas en derechos humanos, —realizadas por personas/entidades expertas independientes y de acceso público— en todas las fases del ciclo de vida de estas tecnologías.
- Sujetar a la cooperación internacional para el desarrollo y el despliegue de sistemas de inteligencia artificial a evaluaciones previas de impacto en Derechos Humanos y ambiental y responder a estrictos criterios de transparencia y rendición de cuentas.

3. Diálogo inclusivo y desarrollo tecnológico ético

- Diseñar e implementar plataformas de diálogo multisectorial para consensuar y adoptar mejores prácticas que fortalezcan una infraestructura regulatoria y de política pública que proteja los derechos a la libertad de expresión, a la reunión pacífica, a la asociación y participación política —tanto en línea como fuera de línea. Esta infraestructura debe prevenir restricciones indebidas, vigilancia arbitraria o censura, especialmente en contextos de protesta social o movilización ciudadana.
- Promover diálogos multisectoriales sobre ciberseguridad, protección de datos y el establecimiento de controles judiciales para prevenir el uso ilegítimo de tecnologías de vigilancia. Es fundamental que estos espacios de diálogos cuenten con la participación activa y representativa de las comunidades afectadas o que podrían verse afectadas de

manera diferenciada, incluyendo a aquellas que históricamente han sido excluidas. También debe asignarse el tiempo y recursos suficientes para asegurar debates significativos y productivos.

- Diseñar e implementar programas de financiación y políticas públicas que condicionen el apoyo a la investigación, diseño y desarrollo de la inteligencia artificial a la integración demostrable de criterios de diversidad, equidad e inclusión, priorizando una perspectiva de género interseccional. Esto debe incluir la exigencia de equipos de desarrollo diversos, la evaluación de sesgos algorítmicos mediante auditorías independientes y la certificación de sistemas de IA que cumplan con estándares de equidad, así como el establecimiento de incentivos efectivos que promuevan activamente la incorporación de estos criterios desde las etapas más tempranas del ciclo de vida tecnológico.

Firman este documento las siguientes organizaciones:

ARTICLE 19, Oficina para México y Centroamérica
CELE - Centro de Estudios en Libertad de Expresión y Acceso a la Información
Derechos Digitales
Electronic Frontier
Foundation Wikimedia
Foundation Usuarios
Digitales
Fundación InternetBolivia.org
Sursiendo, Comunicación y Cultura Digital
Transparencia Electoral
IPANDETEC
Cooperativa Tierra Común
Digital Technology for Democracy Lab, University of Virginia
TEDIC
Conectas Direitos Humanos
Cooperativa Sula Batsú
Fundación Escuela Latinoamericana de Redes, “EsLaRed”
ANDI - Comunicação e Direitos
Observatorio de Derechos Informático Argentino (O.D.I.A.)
Taller de Comunicación Mujer
R3D: Red en Defensa de los Derechos Digitales
ONG Amaranta
Centro LATAM Digital
Fundación Huaira
Red Feminista de Investigación en Inteligencia Artificial
Consorcio Al Sur
MINGAnet, por el cuidado de la Paz y la Vida