

- Presentación de información
a la Relatoría Especial de
Derechos Económicos,
● Sociales, Culturales y
Ambientales de la Comisión
Interamericana de Derechos
Humanos sobre la situación
de los Derechos Económicos,
Sociales, Culturales y
● Ambientales en la región**

**Información presentada conjuntamente
por TEDIC, InternetLab, Derechos
Digitales, Fundación Karisma, Dejusticia,
la Asociación por los Derechos Civiles y
Privacy International**

Noviembre de 2019



INTRODUCCIÓN

TEDIC, InternetLab, Derechos Digitales, la Fundación Karisma, Dejusticia, la Asociación por los Derechos Civiles y Privacy International¹ acogen el llamado de la Relatoría Especial sobre Derechos Económicos, Sociales, Culturales y Ambientales (DESCA) de la Comisión Interamericana de Derechos Humanos (CIDH) de enviar información para la elaboración del Informe Anual sobre DESCA del año 2019, que se presentará ante la Organización de los Estados Americanos (OEA) en 2020.

El objeto de este documento es describir acontecimientos ocurridos en la región en áreas claves de interés que los coautores de la presentación han observado en relación con la realización progresiva de los Derechos Económicos, Sociales, Culturales y Ambientales (DESCA), especialmente respecto al uso de datos y tecnología en conexión con el acceso y el goce de estos derechos.

¹ Al final del documento puede consultarse información adicional sobre cada una de las organizaciones que hacen esta presentación conjunta de información.

ÁREAS CLAVES DE INTERÉS

A continuación, describimos algunas de las principales áreas de preocupación que hemos visto surgir en la región y que recomendaríamos que la Relatoría Especial sobre ESCER de la CIDH abordara y explorara como parte de su mandato e informe anual para el año 2019.

1. Digitalización y centralización de la gestión de los servicios públicos

Los sistemas de servicios públicos digitales han estado surgiendo desde finales de la década de los noventa, sin embargo, en la última década, debido al avance de la tecnología y la capacidad para tratar y explotar datos, aumenta cada vez más la capacidad para recopilar, procesar y reunir inteligencia, lo que es preocupante en vista del rápido avance hacia la digitalización y la centralización de todos los servicios públicos.

En Colombia, existen varios sistemas digitales para gestionar el acceso a servicios públicos como la salud y programas sociales –la carpeta ciudadana² y el Sistema de Identificación de Potenciales Beneficiarios de Programas Sociales (SISBEN)³– que sirven para identificar a las personas que reúnen los requisitos para ser beneficiarios de los programas sociales, entre otros. Los antecedentes del desarrollo de un sistema digital de historias clínicas muestran la prioridad de la digitalización, incluida la retención, el análisis y la reutilización de los datos personales de los ciudadanos con el propósito de explotarlos sin tener en cuenta, o con mínima consideración, del efecto que esto tendría sobre los ciudadanos y sus derechos.⁴

En Paraguay, el Estado reconoce que el Internet es un instrumento importante que puede facilitar los procesos de gestión pública o fortalecer ciertas políticas públicas frente a temáticas como la salud, la educación y el trabajo. La combinación del proyecto Agenda Digital y del eje estratégico “Digitalización del sistema de información de salud” del Ministerio de Salud Pública y Bienestar Social, parece indicar la intención del Gobierno de incorporar el Historial Clínico Electrónico, sin antes haberse asegurado de que el ordenamiento jurídico paraguayo ofrezca garantías adecuadas que protejan eficazmente los datos sensibles almacenados en el sistema.⁵ La digitalización del acceso a los servicios públicos plantea serias inquietudes sobre la exclusión y la discriminación. El Comité de Derechos Económicos, Sociales y Culturales de la ONU, en 2015, en su cuarto informe periódico sobre Paraguay, expresó su preocupación por la ausencia de un mecanismo eficaz para obtener el consentimiento previo, libre e informado de los pueblos indígenas en relación con la toma de decisiones que podrían afectar el ejercicio de sus derechos económicos, sociales y culturales.⁶ Según una

² Para más información ver <https://www.mintic.gov.co/portal/inicio/7229:Carpeta-Ciudadana>

³ Para más información ver <https://www.sisben.gov.co/sisben/Paginas/Que-es.aspx>

⁴ López, J. (2019), *Servicios Ciudadanos Digitales e Historia Clínica Electrónica*, Fundación Karisma.

⁵ Ver <https://www.mspbs.gov.py/dependencias/portal/adjunto/d4d287-MSPyBSPrioridadesInstitucionales.pdf>

⁶ Comité de Derechos Económicos, Sociales y Culturales de la ONU, 20 de marzo de 2015, E/C.12/PRY/CO/4. Disponible en https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=E/C.12/PRY/CO/4&Lang=Sp].

investigación de la UNICEF de 2011, que estudió el acceso a la tecnología en zonas correspondientes a pueblos indígenas, se concluyó que el 96,5% de la población no tiene computadoras.⁷ No existe información actualizada, pero tampoco hay políticas públicas ni empresariales relacionadas con la modificación de las cifras de acceso a Internet y sobre el acervo cultural en línea, ni hay indicadores relativos a Paraguay para mostrar que se logró avanzar la penetración del Internet en el país.

En Brasil, desde 2016, la integración y el intercambio entre las bases de datos de las instituciones públicas se ha facilitado mediante decretos emitidos por el gobierno federal para promover controles más estrictos al proceso de elegibilidad y preservar el acceso a los beneficios de la asistencia social, el trabajo y la seguridad social. Este período, que se caracterizó por la presión de reducir el gasto público –como lo refleja y constitucionaliza la limitación de gasto de 20 años– estuvo marcado por una intensificación del monitoreo, que fue posible gracias al cruce de volúmenes cada vez más grandes de datos, para lo cual se prescindió de acuerdos y se simplificaron los formularios utilizados para solicitar información (Decreto 8.789/2016). Más recientemente, además de la nueva reglamentación del intercambio de datos (Decreto 10.046/2019), se estableció el Registro Base de Ciudadanos. Se trata de una base de referencia de información sobre los ciudadanos desarrollada para las agencias y las entidades del poder ejecutivo federal, a la que se espera que se integren las bases de datos alimentadas por los servicios públicos.⁸ Este Registro contendrá una gran variedad de datos personales generados y recogidos por el Estado en el transcurso de la ejecución e implementación de diferentes políticas públicas, incluidos datos sobre la salud y datos biométricos. Solo los “atributos genéticos” están excluidos del Registro, de acuerdo con lo previsto en el párrafo 6 del artículo 18 del Decreto 10.046/2019. Esto constituye una grave amenaza para la privacidad de las personas, ya que los decretos emitidos en 2019 suponen el riesgo de permitir nuevos niveles de control y discriminación como resultado del acceso facilitado otorgado a las entidades gubernamentales encargadas de aprobar las solicitudes de beneficios sociales o incluso subsidios públicos educativos o culturales a datos sensibles. Esta preocupación se agudiza en el contexto actual, dado que las autoridades federales han declarado abiertamente su intención de limitar algunos tipos de proyectos científicos y culturales,⁹ y cuestiones como el género, la afiliación política y la religión podrían influir sobre estas decisiones.¹⁰

⁷ UNICEF Paraguay, *Escuelas de comunidades indígenas en Paraguay. Análisis de datos 2006-2011*, Noviembre de 2015. Disponible en <https://www.unicef.org/paraguay/informes/escuelas-de-comunidades-ind%C3%ADgenas-en-paraguay-an%C3%A1lisis-de-datos-2006-2011>

⁸ Ramiro, A., *Novas regras põem em risco a privacidade e autonomia de centenas de milhões no Brasil*, 25 de octubre de 2019. Disponible en <https://www.derechosdigitales.org/13961/risco-a-privacidade-de-milhoes-no-brasil/>

⁹ Rodas, S., *MPF move ação contra ministro por censura a projetos LGBT em edital da Ancine*, 2 de octubre de 2019. Disponible en <https://www.conjur.com.br/2019-out-02/mpf-move-acao-ministro-censura-projetos-lgbt>

¹⁰ Ver Chade, J., *Secretário diz na Unesco que arte brasileira servia a “projeto absolutista”*, UOL Noticias, 20 de noviembre de 2019. Disponible en <https://noticias.uol.com.br/colunas/jamil-chade/2019/11/20/secretario-diz-na-unesco-que-arte-brasileira-servia-a-projeto-absolutista.htm?cmpid=copiaecola>; Jeantet, D., *Culture war underway in Brazil as financing becomes tool for censorship*, Buenos Aires Times, 5 de noviembre de 2011. Disponible en <https://www.batimes.com.ar/news/culture/censorship-or-caution-culture-war-burns-in-brazil-as-government-pulls-financing-from-another-play.phtml>

II. La identificación como requisito para acceder a los servicios públicos

Los sistemas de identidad digital plantean algunas interrogantes claves en relación a los derechos de las personas, la protección de su autonomía y dignidad, y con la seguridad e integridad de los datos y la infraestructura establecida.¹¹

Nos preocupa la práctica que está surgiendo de conectar la identidad nacional con los programas de protección social y, en particular, de hacer que la primera sea un requisito para la segunda. Por ejemplo, en Chile, se expide un número de 9 dígitos como parte del proceso de registro de nacimientos: el RUN (Rol Único Nacional). Este número figura en el documento de identidad chileno. Sin embargo, ese mismo número es más conocido como el "RUT" (Rol Único Tributario) –el RUT de un chileno es idéntico a su RUN. Tener un número RUT es necesario para realizar diferentes actividades, desde abrir una cuenta bancaria hasta obtener un seguro médico. También es necesario para firmar la mayoría de los contratos jurídicos, incluidos los de empleo, vivienda y matrimonio. Este requisito obligatorio es excluyente¹² y está siendo cuestionado por la sociedad civil en Chile.¹³

III. El uso de la biometría

Es cada vez más frecuente que la tecnología biométrica se integre a los programas de protección social¹⁴ y a otros programas gubernamentales, como los de policía y orden público. Las justificaciones son variadas, pero a menudo incluyen la transparencia, la eficiencia, la prevención del fraude, la duplicación e incluso el empoderamiento de las personas.

La implementación del denominado "Sistema Biométrico para la Seguridad Alimentaria" en Venezuela requiere que los ciudadanos verifiquen su identidad con sus huellas dactilares para adquirir alimentos, productos de higiene y medicamentos.¹⁵ Este sistema ha dado lugar a quejas de discriminación contra extranjeros, documentados e indocumentados, y personas transgénero.¹⁶ La situación es especialmente preocupante si se tiene en cuenta la escasez de bienes esenciales y la crisis humanitaria cada vez más aguda que afecta primordialmente los derechos a la alimentación y a la salud de las poblaciones más vulnerables.¹⁷

¹¹ Para más información ver <https://privacyinternational.org/topics/identity>

¹² Privacy International, *Exclusion and identity: Life without ID*, 14 de diciembre de 2018. Disponible en <https://privacyinternational.org/feature/2544/exclusion-and-identity-life-without-id>

¹³ Para obtener más información sobre la campaña #NodoymiRUT que lidera la Fundación Datos Protegidos, ver <https://datosprotegidos.org/no-doy-mi-rut/>

¹⁴ Sepúlveda Carmona, M., *Is biometric technology in social protection programmes illegal or arbitrary? An analysis of privacy and data protection?*, Extensión de la Seguridad Social, Departamento de Protección Social, Oficina Internacional del Trabajo, Working Paper No. 59. Disponible en https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---soc_sec/documents/publication/wcms_631504.pdf

¹⁵ Díaz, M., *Tu huella digital por un kilo de harina: biométrica y privacidad en Venezuela*, Digital Rights Lac, 16 de diciembre de 2016. Disponible en <https://www.digitalrightslac.net/es/tu-huella-digital-por-un-kilo-de-harina-biometrica-y-privacidad-en-venezuela/>

¹⁶ Díaz, M., *El Cuerpo Como Dato*, Derechos Digitales, junio de 2018. Disponible en https://www.derechosdigitales.org/wp-content/uploads/cuerpo_DATO.pdf

¹⁷ *Bachelet: Las nuevas sanciones de EE.UU. a Venezuela pueden tener un impacto severo en la población*, Noticias ONU, 8 de agosto de 2019. Disponible en <https://news.un.org/es/story/2019/08/1460361>

Otro uso de la biometría que se ha extendido rápidamente en la región es la utilización de sistemas de reconocimiento facial. Estos han sido implementados, por ejemplo, en Paraguay.¹⁸ En 2019, el país implantó un nuevo sistema para digitalizar la utilización y el pago del transporte público. La justificación ofrecida para poner en marcha el proyecto fue mejorar la transparencia y el acceso a los servicios públicos.¹⁹

Del mismo modo, en São Paulo, en 2017, se empezaron a utilizar cámaras de reconocimiento facial en el sistema de transporte público en aras de apoyar la prevención de fraudes en el uso de los beneficios sociales relacionados con el transporte, como los descuentos para las personas mayores, los estudiantes y las personas con discapacidades. Desde entonces, el sistema ha bloqueado más de trescientas mil tarjetas argumentando que fueron utilizadas indebidamente, esto es, que no fueron utilizadas por sus titulares originales.²⁰ Paralelamente, el Gobierno Municipal ha anunciado la suspensión total de las tarjetas anónimas²¹ y ha implementado medidas que obligan a registrarlas con datos de identificación únicos y residenciales.²² Este tipo de medidas puede afectar al acceso a los servicios del transporte público de las personas que no están registradas, como las personas sin hogar y los inmigrantes. En una ciudad tan grande como São Paulo, las tarjetas que permiten viajar en diferentes tipos de transporte con descuento son fundamentales para que la mayoría de la población pueda acudir al trabajo, a la escuela y a actividades culturales. Bloquear o dificultar el acceso al transporte puede afectar considerablemente la vida y el desarrollo de las personas.

En Argentina, en abril de 2019, la Ciudad de Buenos Aires lanzó un nuevo sistema facial que se iría extendiendo gradualmente por todos los espacios públicos a través de cámaras CCTV.²³ Además de ser desproporcionado, el sistema plantea serias y alarmantes inquietudes sobre el efecto que tendría sobre el goce de las libertades y derechos fundamentales en los espacios públicos, tal como se plantea en la demanda de inconstitucionalidad presentada por la Asociación por los Derechos Civiles (ADC).²⁴

¹⁸ TEDIC, *¿Quién vigila al vigilante? Reconocimiento Facial en Asunción*, 16 de septiembre 2019. Disponible en <https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/>

¹⁹ TEDIC, *El billete electrónico, ¿nuestros derechos están en juego?*, 20 de marzo 2019. Disponible en <https://www.tedic.org/el-billete-electronico-nuestros-derechos-estan-en-juegos/>

²⁰ Tecmundo, *Reconhecimento facial bloqueia 331 mil Bilhetes Únicos em SP*, 12 de junio 2019. Disponible en <https://www.tecmundo.com.br/seguranca/142472-paulo-bloqueia-331-mil-bilhetes-unicos-reconhecimento-facial.htm>

²¹ Dia, B., *Venda de Bilhete Único anônimo será suspenso*, diz secretário de Transporte de SP, G1, 7 de junio 2018. Disponible en <https://g1.globo.com/sp/sao-paulo/noticia/bilhete-unico-anonimo-sera-suspenso-diz-secretario-de-transportes-de-sp.ghtml>

²² Vicente, J. P., *Mudanças no Bilhete Único acendem alerta sobre coleta indevida de dados*, Vice, Motherboard, 25 de febrero de 2019. Disponible en https://www.vice.com/pt_br/article/paqa7n/mudancas-no-bilhete-unico-acendem-alerta-sobre-coleta-indevida-de-dados

²³ Uccifferi, L., *#ConMiCaraNo: Reconocimiento facial en la Ciudad de Buenos Aires*, ADC, 23 de mayo de 2019. Disponible en <https://adc.org.ar/2019/05/23/con-mi-cara-no-reconocimiento-facial-en-la-ciudad-de-buenos-aires/>

²⁴ ADC, *El reconocimiento facial para vigilancia no pertenece a nuestro espacio público*, 6 de noviembre de 2019. Disponible en <https://adc.org.ar/2019/11/06/el-reconocimiento-facial-para-vigilancia-no-pertenece-a-nuestro-espacio-publico/>

En Colombia, las Autoridades de Migración implementaron un escáner de iris como una alternativa al control de pasaportes que habitualmente realizan los funcionarios de migración. El sistema se estableció sin que se discutiera adecuadamente y sin pruebas de su necesidad, mediante órdenes administrativas que eludieron una discusión en el Congreso. Entretanto, la Policía utiliza escáneres portátiles de huellas dactilares para verificar la identidad de los ciudadanos durante los registros callejeros que se basan en los datos biométricos de la Registraduría Nacional del Estado Civil.²⁵

También hemos observado la implantación de sistemas de votación electrónicos y biométricos en países como Brasil, entre otros. La implantación de la validación biométrica para votar en Brasil, donde ya operan sistemas de votación electrónica, se está desarrollando por fases e impidió el voto de más de tres millones de ciudadanos en las últimas elecciones que no registraron sus huellas dactilares a tiempo.²⁶ Además de afectar su derecho al voto, la anulación de los documentos de votación en Brasil, en donde el voto es obligatorio para todos los ciudadanos mayores de dieciocho años, impide que las personas ejerzan derechos como obtener o renovar un pasaporte o solicitar beneficios sociales como "Bolsa Familia".²⁷ Se prevé que en 2022 se habrá instalado completamente la tecnología biométrica.

IV. Digital, IA y automatización

En algunos países, los gobiernos están adoptando servicios públicos digitales que buscan integrar cada vez más sistemas automatizados en sus diseños, algunos de los cuales operan de forma paralela a elementos no automatizados.

Una de las áreas en la que se está aplicando la inteligencia artificial es para identificar a menores que están en peligro de ser maltratados antes de que sufran cualquier daño. Se han implementado programas automatizados que buscan identificar a las familias que necesitan atención. En 2019, Chile empezó la implementación piloto de una herramienta que busca detectar a los menores y adolescentes en situación de riesgo.²⁸ De acuerdo con el Ministerio de Desarrollo Social y Familia, Alerta Niñez es una herramienta preventiva que "identifica el conjunto de condiciones individuales, familiares, del entorno y de los pares de los niños y niñas y adolescentes, que tienden a presentarse cuando existe un riesgo de vulneración". Mediante el tratamiento estadístico de grandes cantidades de datos tomados de entidades públicas, el sistema asigna un puntaje individualizado a cada menor y a cada adolescente basado en sus probabilidades de que se vulneren sus derechos.

²⁵ Fundación Karisma, *Biometría en el Estado colombiano*, 2 de julio de 2019. Disponible en <https://archive.org/details/biometria2>

²⁶ DW, *STF mantém cancelados títulos de eleitor sem biometria*, 26 de septiembre de 2018. Disponible en <https://www.dw.com/pt-br/stf-mant%C3%A9m-cancelados-t%C3%ADtulos-de-eleitor-sem-biometria/a-45652801>

²⁷ Platonow, *Cadastramento biométrico é feito por 72% dos eleitores*, Agência Brasil, 6 de septiembre de 2019. Disponible en <http://agenciabrasil.ebc.com.br/justica/noticia/2019-09/cadastramento-biometrico-e-feito-por-72-dos-eleitores>

²⁸ Ver Ministerio de Desarrollo Social y Familia. Disponible en https://cdn.digital.gob.cl/filer_public/8a/e7/8ae7acf1-230b-45b3-806f-4cd6d4d837fb/11_mindesarrollosocial-f.pdf

Esta es una iniciativa invasiva para recopilar datos sensibles de menores de edad que implica un alto riesgo de exacerbar los prejuicios y la estigmatización hacia grupos históricamente vulnerables, en particular los hogares monoparentales encabezados por mujeres y, posiblemente, las familias no binarias. Asimismo, estos procesos suponen la transferencia de datos personales a terceros y la posibilidad de que los mismos sean utilizados para fines distintos a los acordados, sin que existan fundamentos y garantías jurídicas que aseguren que la información que se genere no será utilizada en el futuro para otros fines, como, por ejemplo, para iniciativas de vigilancia policial predictivas o para eventuales posibilidades de empleo, lo que podría conducir a la discriminación de los menores y los familiares cobijados por este programa.

En Paraguay, la automatización ha sido implementada en la gestión de los servicios públicos. El proyecto del Ministerio de Trabajo denominado "Para Empleo" propone un sistema de inteligencia artificial para la búsqueda de trabajo. Actualmente no existe mucha información a disposición del público, sin embargo, será importante conocer las especificaciones técnicas y las evaluaciones de riesgo sobre protección de datos y derechos humanos que se hayan desarrollado (si las hubo) para sustentar la implementación de dicho sistema.²⁹

En Colombia, se han anunciado varios proyectos que emplean la inteligencia artificial. La Corte Constitucional ha contactado a proveedores privados con el objetivo de implementar un sistema de lectura y clasificación de las numerosas acciones de tutela que la Corte debe evaluar para seleccionar los casos que precisan de su intervención.³⁰ La Fiscalía General de la Nación ha anunciado un sistema de predicción de reincidencia para adoptar decisiones sobre la detención preventiva con el apoyo de modelos de aprendizaje automático o *machine learning*.³¹ El Gobierno colombiano también planea desarrollar el sistema de puntaje (SISBEN) y los datos de los beneficiarios con el fin de identificar a las personas que supuestamente abusan del sistema y desarrollar negocios de inteligencia artificial con estos datos. El sistema SISBEN se utiliza en Colombia desde 1994 y califica el nivel de pobreza de las personas en una escala de cero a cien, de los más pobres a los más ricos. Los datos se han obtenido a través de la realización de encuestas exhaustivas a los posibles beneficiarios. Sin embargo, la última versión del programa busca conectar y analizar varias bases de datos oficiales y financieras para excluir a las personas de acuerdo con su nivel de ingresos. Adicionalmente, la última versión del SISBEN ofrece sus datos a empresas

²⁹ IP, *Paraguay presenta plataforma de inteligencia artificial de búsqueda de empleo*, 6 de diciembre de 2018. Disponible en <https://www.ip.gov.py/ip/gobierno-lanza-plataforma-de-inteligencia-artificial-de-busqueda-de-empleo/>

³⁰ Camacho, L., *¿Cómo implementar Inteligencia Artificial en la Corte Constitucional? la pregunta que nos montó en una colaboración academia, sociedad civil y la propia corte*, Fundación Karisma, 2 de septiembre de 2019. Disponible en <https://stats.karisma.org.co/como-implementar-inteligencia-artificial-en-la-corte-constitucional-la-pregunta-que-nos-monto-en-una-colaboracion-academia-sociedad-civil-y-la-propia-corte/>

³¹ Ver Fiscalía General de la Nación, *Fiscalía implementa herramienta 'Prisma' para lograr de manera más efectiva que personas con alto riesgo de reincidencia criminal sean cobijadas con medida de aseguramiento*, 29 de mayo de 2019. Disponible en <https://www.fiscalia.gov.co/colombia/noticias/fiscalia-implementa-herramienta-prisma-para-lograr-de-manera-mas-efectiva-que-personas-con-alto-riesgo-de-reincidencia-criminal-sean-cobijadas-con-medida-de-aseguramiento/>

que proponen modelos para predecir el comportamiento de quienes “defraudan” al sistema.³²

V. *La economía digital y los derechos laborales*

Algunos desarrollos tecnológicos de la arquitectura abierta del Internet han permitido la aparición de nuevas empresas que prestan servicios de intermediación entre proveedores de servicios y posibles clientes. Estas plataformas acentúan las transformaciones de las relaciones entre el trabajo y el capital en las sociedades postindustriales. En sociedades con altas tasas de desempleo, altos niveles de informalidad y flexibilidad en las normas de protección laboral, el surgimiento de estas plataformas –apoyadas en esquemas empresariales basados en la innovación tecnológica y que operan bajo el modelo de la intermediación– representa nuevos riesgos para el goce efectivo de los derechos a condiciones de trabajo dignas, salarios justos y a la seguridad social para las personas que, para ofrecer su fuerza de trabajo, se suscriben, afilian y usan estas plataformas. La escala (el elevado número de usuarios e interacciones sociales que fomenta la plataforma) y la ausencia de regulación y supervisión estatal incrementan estos riesgos.

Asimismo, el desarrollo de aplicaciones (apps) que ofrecen, en línea y sin intervención humana directa, servicios similares a los servicios que ofrecen análogamente trabajadores especializados, representa un nuevo riesgo para el derecho humano al trabajo. Tales aplicaciones utilizan y tratan información de dominio público a través de diferentes medios (*big data*, algoritmos, etc.) y de diferentes ramas de conocimiento (médico, contable, jurídico, lingüístico, etc.) e incluso utilizan y tratan información que inicialmente fue aportada por profesionales de estas ramas, para luego, con base en la misma, y sin necesidad de intervención humana directa, sustituir la pericia y labor de estos profesionales.

VI. *Tecnología educativa*

Los gobiernos están mostrando cada vez más interés en integrar lo digital a la educación, con la tecnología como el factor clave que impulsa la mejora de la calidad de la educación. Gradualmente, la empresa privada se ha convertido en la responsable de suministrar las plataformas educativas digitales y, en algunos casos, crear los expedientes digitales de los estudiantes. Estos desarrollos se observan en Brasil, con el uso de Google Apps con fines educativos en escuelas y universidades.³³

Esto es preocupante por el aumento de la recopilación de datos sobre menores, lo que permite la creación de perfiles y registros digitales que seguirán existiendo aun mucho después de que los menores terminen su educación y, además, pueden ser usados para vigilar a los estudiantes y a los profesores.

³² Para más información ver <https://www.sisben.gov.co/Documents/Compes%20IV/6285-CONPES%203877.pdf>

³³ Oliveira, F., *Escolas na mira das corporações da internet*, LAVITS, 4 de junio de 2019. Disponible en <http://lavits.org/escolas-na-mira-das-corporacoes-da-internet/?lang=pt>

VII. *Derechos sexuales y reproductivos*

Los derechos sexuales y reproductivos, que son parte de los DESCAs, incluyen el derecho a acceder a la anticoncepción, el derecho al aborto seguro y legal, el derecho a acceder a la información de salud sexual, incluida la anticoncepción y el aborto, y otros servicios de salud reproductiva. La explotación de los datos por parte de empresas que busca coartar su ejercicio es una amenaza para estos derechos. Por ejemplo, Heartbeat International es una organización afiliada con sede en Estados Unidos que trabaja para restringir los derechos sexuales y reproductivos, entre otros, en muchos Estados miembros de la OEA. La visión declarada de esta organización es "hacer que el aborto sea indeseable en el presente e impensable para las generaciones futuras".³⁴

Heartbeat International afirma tener afiliados en 24 estados miembros de la OEA, entre ellos: Argentina, Bahamas, Belice, Bolivia, Brasil, Canadá, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Estados Unidos, Guatemala, Haití, Honduras, México, Nicaragua, Panamá, Paraguay, Perú, República Dominicana, Trinidad y Tobago, Uruguay y Venezuela.³⁵

Heartbeat International está desarrollando y promoviendo herramientas explotadoras que utilizan grandes cantidades de datos, las cuales promueven entre sus afiliados. Por ejemplo, la organización ha desarrollado una "solución para la administración de centros" llamada Next Level, que al parecer recopila grandes cantidades de información sobre las personas que visitan los centros de embarazos en crisis.³⁶ El sistema, que se puede ver en un video promocional en el sitio web de Next Level, recopila diferentes tipos de información como el nombre, la dirección de la residencia, la dirección de correo electrónico, el grupo étnico, el estado civil, la situación de vivienda, el nivel educativo, la fuente de ingresos, el consumo de alcohol, cigarrillos y drogas, los medicamentos consumidos y la historia clínica, el historial de enfermedades de transmisión sexual, el nombre de la persona/organización que remite, síntomas e historial del embarazo, información sobre exámenes médicos y, eventualmente, hasta imágenes de ecografías.³⁷ Next Level comercializa el software como un sistema que "[h]ace posible la recopilación fluida de datos para los centros de embarazos", pero parece que los datos recopilados por el sistema son enviados a Estados Unidos.³⁸

Heartbeat desarrolló Option Line, que es un chat box y una línea de ayuda.³⁹ Usualmente está disponible en los sitios web de Extend y otros centros de crisis de embarazo. Antes de empezar el chat, la persona debe proporcionar información sobre su ubicación, si tiene una "mentalidad abortiva", el rango de edad y otros datos personales. No está claro a quién se envían estos datos y los datos del chat. Es preocupante la casi absoluta falta de transparencia sobre cómo redes en

³⁴ Ver Heartbeat, About us. Disponible en <https://www.heartbeatinternational.org/about-us>

³⁵ Ver Heartbeat, Worldwide Directory of Pregnancy Help. Disponible en <https://www.heartbeatinternational.org/worldwide-directory>

³⁶ Privacy International, *How anti-abortion activism is exploiting data*, 22 de julio de 2019. Disponible en <https://privacyinternational.org/long-read/3096/how-anti-abortion-activism-exploiting-data>

³⁷ Ver <https://www.nextlevelcms.com/>

³⁸ Ver <https://www.heartbeatinternational.org/next-level-supporter>

³⁹ Privacy International, *How anti-abortion activism is exploiting data*, 22 de julio de 2019. Disponible en <https://privacyinternational.org/long-read/3096/how-anti-abortion-activism-exploiting-data>

contra de los derechos sexuales y reproductivos, como Heartbeat International, están utilizando y compartiendo datos. Existe la posibilidad de que los datos sean usados de maneras que no anticiparon ni aprobaron las personas que los suministraron, incluidos usos que podrían minar sus derechos reproductivos. Por ende, son esenciales la privacidad y una fuerte protección de los datos, en muchos sentidos, para garantizar que las personas puedan ejercer sus derechos reproductivos. Es importante arrojar luz sobre las tecnologías que se están desarrollando para rastrear a quienes buscan ayuda médica en línea.

En Argentina, en 2017, la provincia de Salta firmó un acuerdo con Microsoft para utilizar la inteligencia artificial en la prevención del embarazo adolescente y la deserción escolar.⁴⁰ Según la empresa, basados en los datos recogidos entre poblaciones en situación de vulnerabilidad, “algoritmos inteligentes permiten identificar características en las personas que podrían derivar en alguno de estos problemas [el embarazo adolescente y la deserción escolar] y advierten al gobierno para que puedan trabajar en la prevención de los mismos”. Los datos recogidos son tratados por servidores de Microsoft en todo el mundo y el tratamiento se enfoca específicamente en los adolescentes que han sido identificados como personas en riesgo, lo que afecta no sólo a su privacidad, sino también su autonomía y genera un gran potencial de discriminación. Básicamente, se trata de un mecanismo para el control de las personas destinatarias en situación de vulnerabilidad, quienes se ven expuestas a intervenciones que no han consentido y que refuerza la vulnerabilidad de personas que se ven privadas incluso de la posibilidad de decidir sobre dichas intervenciones. Aunque se podría argumentar que los datos utilizados para las proyecciones fueron suministrados voluntariamente, es cuestionable que niñas y adolescentes afectadas por estas medidas –o sus guardianes– puedan consentir explícitamente, teniendo en cuenta las consecuencias de proporcionar información concreta sobre sus hábitos sexuales y su posible embarazo. Cabe señalar que Salta fue la última provincia argentina que dejó de impartir educación religiosa en las escuelas públicas después de que la Corte Suprema de Justicia dictara una sentencia en la que reconocía la existencia de vulneraciones de los derechos a la igualdad y a la no discriminación, así como de la privacidad de los ciudadanos. La dependencia de la tecnología que describimos, no es más que una expresión de problemas más amplios para entender las esferas de la autonomía y la privacidad de las personas, con fines políticos.

En Brasil, el Ministerio de Ciudadanía celebró un acuerdo con el Gobierno de Salta y Microsoft para implementar un programa similar. En este caso, aparte de la prevención del embarazo adolescente y la deserción escolar, se propone prever problemáticas como la desnutrición y las enfermedades en la primera infancia. El país sería el quinto de la región en replicar la experiencia argentina. Además de los interrogantes sobre el consentimiento informado y el acceso estatal a información sensible sobre poblaciones en situaciones vulnerables, otras preguntas siguen sin resolver, como sobre los demás usos o las predicciones que

⁴⁰ Microsoft, *Microsoft y el gobierno de Salta firman un acuerdo para aplicar la inteligencia artificial en la prevención de los problemas más urgentes*, News Center LATAM, 7 de junio de 2017. Disponible en <https://news.microsoft.com/es-xl/microsoft-gobierno-salta-firman-acuerdo-aplicar-la-inteligencia-artificial-la-prevencion-los-problemas-mas-urgentes/>

pueden extraerse de estos datos y los riesgos potenciales, teniendo en cuenta que son tratados por Microsoft y los gobiernos que participan en el programa.⁴¹

VIII. Problemáticas contextuales y sistemáticas

Además de las áreas de interés, quisiéramos destacar algunos puntos clave que también deben ser considerados y abordados cuando se exploren las áreas de interés antes mencionadas.

- **La falta de regulación eficaz:** muchos Estados miembros de la OEA no cuentan con un marco jurídico que regule el tratamiento de datos personales, mientras que los Estados miembros que sí cuentan con algún tipo de regulación, no la están haciendo cumplir de manera eficaz. Esto significa que, en general, las actividades de tratamiento de datos de las entidades públicas y privadas no están siendo reguladas. Además, los Estados miembros no adoptan medidas para asegurar el respeto de sus obligaciones en relación con otros derechos humanos, como los principios de no discriminación e igualdad, en el proceso de implementación de soluciones digitales. La falta de salvaguardias que protejan los derechos a la privacidad y a la protección de datos, así como la falta de atención prestada a la seguridad en el despliegue de soluciones digitales que son implementadas apresuradamente para supuestamente facilitar el acceso y la realización de los derechos DESCAs, significa que hoy día las personas se ven obligadas a canjear su privacidad para poder acceder a otros derechos y libertades fundamentales.
- **Los impulsores:** Debe prestarse especial atención a los factores que impulsan el uso de la tecnología para la realización de los derechos económicos, sociales, culturales y medioambientales, ya que, de lo contrario, los mismos sistemas concebidos para facilitar el goce de los derechos fundamentales amplificarán las carencias y las injusticias ya existentes. Los impulsores contextuales incluyen la creciente preocupación por la austeridad y la transparencia, la eficiencia y la gestión financiera, ya que muchas de las soluciones técnicas que usan grandes cantidades de datos son propuestas como soluciones que permiten disminuir los gastos y apoyan, entre otras, las medidas de austeridad.
- **Riesgos y daños:** La digitalización de los servicios públicos puede afectar negativamente a las personas y comunidades que ya están en situación de desventaja, incluidas quienes se encuentran en situación de desventaja debido a su condición económica, social, de clase o jurídica, entre otros factores; quienes dependen del Estado para su sustento y el de sus familias y dependientes; y las comunidades y personas que ya estaban marginadas y han sido las más duramente golpeadas por las medidas de austeridad y los recortes de los beneficios, como las mujeres, las minorías étnicas, las personas LGTBIQ y de género fluido y los migrantes (regulares e irregulares).

⁴¹ Venturini, J., *Vigilancia, control social e inequidad: la tecnología refuerza vulnerabilidades estructurales en América Latina*, Derechos Digitales, 10 de octubre 2019. Disponible: <https://www.derechosdigitales.org/13900/vigilancia-control-social-e-inequidad/>

Ya han sido denunciados y documentados algunos de estos riesgos, incluida la estigmatización, la discriminación y la exposición a la vigilancia del Estado y de las empresas.

- ***El papel del sector privado:*** Debe prestarse atención al papel de la industria en este sector. La industria no sólo suministra soluciones a los gobiernos, sino que, a través de la prestación de sus propios servicios, también alimenta el ecosistema general de la explotación de datos.⁴² Las empresas no solo deben ser transparentes sobre cómo funcionan en la práctica sus modelos de negocio, es decir, el diseño de sus sistemas y las soluciones que ofrecen a los gobiernos, sino que también deben separar y aislar estas actividades de las otras áreas de sus modelos de negocio e intereses.

CONCLUSIONES

El uso de la tecnología y los datos para la realización de los derechos económicos, sociales, culturales y ambientales plantea, entre otros puntos, interrogantes clave en relación con la protección, el respeto y la promoción del derecho a la privacidad consagrado en el artículo 11 de la Convención Americana sobre Derechos Humanos, en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y en el artículo 12 de la Declaración Universal de Derechos Humanos. Puesto que los sistemas que están siendo implementados interfieren con la privacidad de las personas, deben cumplir el principio de legalidad y, además, ser necesarios y proporcionales al objetivo legítimo que pretenden alcanzar. Aparte de la falta de protección de las personas y sus datos cuando interactúan con los sistemas implantados, éstos también tienen repercusiones en la no discriminación y la igualdad.⁴³

En su informe anual a la Asamblea General de las Naciones Unidas sobre el estado de bienestar digital y los derechos humanos,⁴⁴ el Relator Especial de las Naciones Unidas sobre la extrema pobreza y los derechos humanos presentó tres observaciones que, como se destaca en las áreas de interés descritas en esta presentación de información, también deberían ser tenidas en cuenta por la Relatoría Especial sobre Derechos Económicos, Sociales, Culturales y Ambientales (DESCA), incluido que los gobiernos corren el riesgo de “desembocar, sin ser conscientes de ello, en una distopía de bienestar digital”, que “las grandes empresas tecnológicas [a menudo llamadas ‘big tech’] actúan en una esfera en la que los derechos humanos están prácticamente ausentes”, y que “en lugar de obsesionarse con el fraude, el ahorro, las sanciones y las definiciones de eficiencia determinadas por el mercado, el punto de partida sea cómo transformar los

⁴² Ver la campaña de Privacy International “Tell companies to stop exploiting your data!”. Información adicional disponible en <https://privacyinternational.org/campaigns/tell-companies-stop-exploiting-your-data>

⁴³ Ver el trabajo de Privacy International que explora los datos y la tecnología y el acceso a los derechos económicos, sociales y culturales. Información adicional disponible en <https://privacyinternational.org/what-we-do/realise-our-rights-live-dignity>

⁴⁴ A/74/493, 11 de octubre de 2019. Disponible en <https://undocs.org/A/74/493>

presupuestos de asistencia social mediante la tecnología para mejorar el nivel de vida de las personas vulnerables y desfavorecidas”.

Indiscutiblemente, la tecnología puede ayudar a que los gobiernos cumplan su obligación de realizar los derechos económicos, sociales, culturales y ambientales y a que resuelvan algunos de los desafíos fundamentales que enfrentan al hacerlo con el fin de garantizar que las personas y las comunidades vivan con dignidad, pero es necesario tener en cuenta desde el principio las salvaguardas y garantías del debido proceso a fin de identificar y mitigar los riesgos y permitir el acceso a la reparación.

Este primer llamado de la Relatoría Especial sobre los Derechos Económicos, Sociales, Culturales y Ambientales es un importante primer paso, que brinda la oportunidad de dibujar el panorama actual de la situación de los DESCAs en la región. Esperamos que conduzca a la adopción de medidas concretas adicionales que aborden las temáticas planteadas en este documento, y a la adopción de medidas por parte de los gobiernos, la industria y terceros para velar por el respeto, la promoción y la protección de los derechos económicos, sociales, culturales y ambientales en la región.

Una postura firme contra la explotación de datos es esencial para cuestionar la dinámica de poder actual, garantizar la dignidad y la autonomía de las personas y evitar nuevas violaciones de los derechos y las libertades fundamentales.

INFORMACIÓN SOBRE LOS COAUTORES DE LA PRESENTACIÓN

TEDIC

www.tedic.org

TEDIC es una organización sin ánimo de lucro que promueve los derechos humanos en Internet, con sede en Paraguay. Algunas de sus estrategias son: el desarrollo de tecnologías cívicas para el cambio social, el litigio estratégico, la investigación, las campañas y la incidencia política.

Contacto: Maricarmen Sequera, directora ejecutiva, maricarmen@tedic.org

InternetLab

www.internetlab.org.br

InternetLab es un centro de investigación interdisciplinario independiente que promueve el debate académico y la producción de conocimiento en los campos del derecho y la tecnología, especialmente en el campo de Internet. Nuestro objetivo es desarrollar investigaciones interdisciplinarias de alto impacto y promover el diálogo entre académicos, profesionales y formuladores de políticas. Adoptamos un modelo emprendedor sin ánimo de lucro, que refleja nuestro afán de producir investigación académica al igual y con el mismo espíritu que un centro de pensamiento académico. Como un nexo de conocimiento en tecnología,

política pública y ciencias sociales, nuestra agenda de investigación abarca una amplia gama de temas, incluyendo la privacidad, la libertad de expresión, género y la tecnología.

Contacto: Nathalie Fragoso, directora de investigación sobre privacidad y vigilancia, nathalie.fragoso@internetlab.org.br

Derechos Digitales

www.derechosdigitales.org

Derechos Digitales es una organización de alcance latinoamericano, independiente y sin fines de lucro, fundada en 2005 y que tiene como objetivo fundamental el desarrollo, la defensa y la promoción de los derechos humanos en el entorno digital.

Contacto: Jamila Venturini, jamila@derechosdigitales.org

Fundación Karisma

www.karisma.org.co

La Fundación Karisma es una organización de la sociedad civil colombiana que busca responder a las amenazas y oportunidades que plantea la "tecnología para el desarrollo" al ejercicio de los derechos humanos. Karisma se centra en el activismo, incorporando diversas perspectivas legales y técnicas.

Contacto: Juan Diego Castañeda, Researcher, juancastaneda@karisma.org.co

Dejusticia

www.dejusticia.org

Fundada en 2005, Dejusticia es una organización de investigación e incidencia localizado en Colombia que se dedica al fortalecimiento del estado de derecho y a la promoción de la justicia social y los derechos humanos en Colombia y en el Sur Global. Dejusticia promueve el cambio social a través de estudios rigurosos y propuestas de políticas públicas basadas en hechos; adelantando campañas de incidencia en foros de alto impacto; y diseñando e impartiendo programas educativos y de formación.

Contacto: Daniel Ospina Celis, investigador, dospina@dejusticia.org

Asociación por los Derechos Civiles

<https://adc.org.ar/>

La Asociación por los Derechos Civiles (ADC) es una organización no gubernamental, apartidaria y sin fines de lucro con sede en Buenos Aires, que promueve los derechos civiles y sociales en la Argentina y otros países latinoamericanos. Fue fundada en 1995 con el propósito de contribuir a afianzar

una cultura jurídica e institucional que garantice los derechos fundamentales de las personas, sustentada en el respeto por la Constitución y los valores democráticos.

Contacto: Leandro Ucciferri, Senior Project Officer, luciferri@adc.org.ar

Privacy International

www.privacyinternational.org

Privacy International (PI) es una importante organización no gubernamental que promueve la adopción de normativas fuertes a nivel nacional, regional e internacional que garanticen el derecho a la privacidad en todo el mundo. Fundada en 1990 y con sede en Londres, PI cuestiona los excesos de la vigilancia estatal y corporativa para que las personas en todo el mundo puedan gozar de mayor seguridad y libertad gracias a una mayor privacidad personal. Como parte de su esfera de actividades, PI investiga cómo se generan y explotan los datos personales de los individuos y cómo se pueden proteger a través de marcos legales y tecnológicos.

Contacto: Alexandrine Pirlot de Corbion, directora de estrategia

alex@privacyinternational.org

**PRIVACY
INTERNATIONAL**

Privacy International

62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321

www.privacyinternational.org

Twitter @privacyint

Instagram @privacyinternational

UK Registered Charity No. 1147471