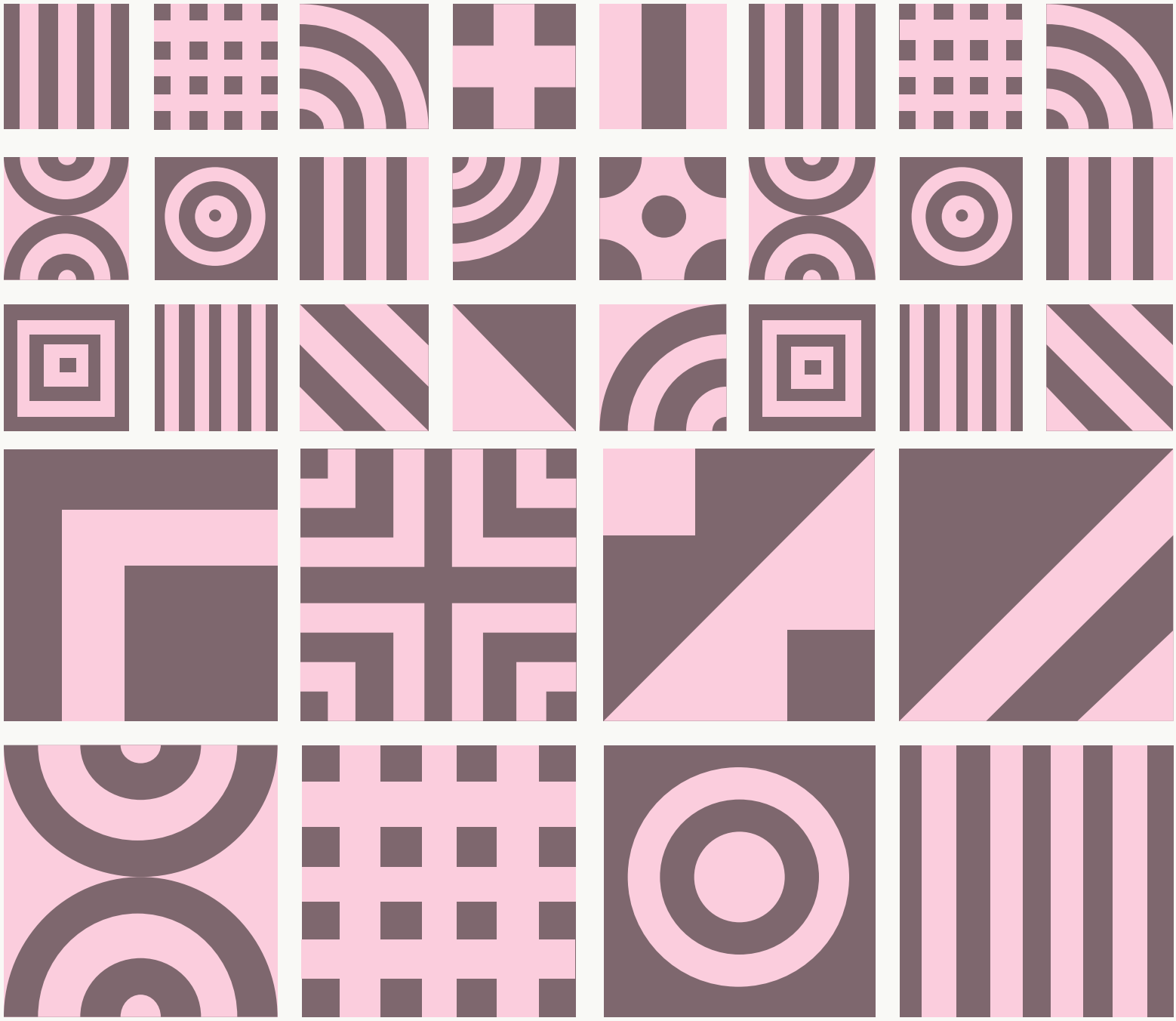

Inteligencia Artificial en el Estado: estudio colectivo sobre experiencias y riesgos para los Derechos Humanos

DERECHOS DIGITALES
América Latina

INTELIGENCIA ARTIFICIAL EN EL ESTADO: ESTUDIO COLECTIVO SOBRE EXPERIENCIAS Y RIESGOS PARA LOS DERECHOS HUMANOS

Este informe fue realizado por Derechos Digitales, organización independiente y sin fines de lucro, fundada en el año 2005, cuya misión es la defensa, promoción y desarrollo de los derechos fundamentales en los entornos digitales en América Latina. Para más información sobre este proyecto, visita https://ia.derechosdigitales.org/.

Supervisión general: Jamila Venturini y Juan Carlos Lara

Autor: Juan Manuel García

Edición: Paloma Lara Castro y Juan Carlos Lara

Traducción al inglés y al portugués: Urgas Traductoras

Diseño: Alter Studio

Noviembre, 2024

INTELIGENCIA ARTIFICIAL EN EL ESTADO: ESTUDIO COLECTIVO SOBRE EXPERIENCIAS Y RIESGOS PARA LOS DERECHOS HUMANOS

INTRODUCCIÓN

I. LA INTELIGENCIA ARTIFICIAL COMO ARTEFACTO SOCIOTÉCNICO

La Inteligencia Artificial ya forma parte de la batería de herramientas a disposición de la función pública para la planificación e implementación de políticas públicas. La frecuente percepción sobre estas tecnologías, enfocada principalmente en su utilidad para eficientizar procesos, tiene una influencia determinante a la hora de decidir aplicarlas al sector público. En ese sentido, dichas herramientas son implementadas para tomar decisiones relativas a, por ejemplo, qué sector poblacional priorizar sobre otro para determinada política; o qué personas pueden, potencialmente, requerir más acompañamiento estatal que otras en determinada situación, entre otros ejemplos de uso. En este sentido, surgen inquietudes respecto de cuáles son las implicancias para el ejercicio de derechos fundamentales del uso de estas tecnologías. Esta situación es común independientemente de las técnicas específicas que caben dentro del paraguas conceptual de la IA, tales como los modelos de procesamiento de lenguaje natural (NLP), aprendizaje automático (ML), sistemas predictivos de riesgo, y procesos de decisión automatizada (ADM)[1].

Con el propósito de conocer más sobre el tema, y aportar evidencia sobre estos procesos, desde 2019, desde Derechos Digitales analizamos esta problemática en el marco del eje programático *Inteligencia Artificial e Inclusión,* donde trabajamos con investigadoras de distintos países de América Latina para analizar en qué áreas utiliza el Estado estas tecnologías, qué particularidades tiene ese uso y cuáles son los riesgos potenciales para

1 Los acrónimos surgen de sus nombres en inglés. Respectivamente, “Natural Language Processing”, “Machine Learning” y “Automated Decision-Making”.

los derechos humanos. Estas investigaciones tomaron la forma de estudios de caso, que fueron desarrollados en función de una metodología que contemplaba múltiples dimensiones de análisis común a todos ellos, con especial interés en el potencial impacto en derechos de las personas. Se trata de estudios exploratorios que buscan aportar evidencia sobre una actividad aún incipiente, pero en aceleración.

El insumo principal para el desarrollo técnico de las tecnologías basadas en inteligencia artificial son los datos. Sin embargo, los estados en América Latina tienen dificultades para mantener prácticas robustas de uso, gestión y almacenamiento de datos, en parte por problemas como la fragmentación de bases de datos, la heterogeneidad en la perspectiva sobre los datos entre dependencias estatales, la diversidad de sistemas informáticos, o la falta de un lenguaje común (Fundar, 2024). Esto representa un problema adicional a la hora de considerar que detrás de los datos utilizados por la IA, en el marco de la gestión estatal, hay personas que buscan trabajo, que están en una situación de necesidad que permitiría recibir una pensión estatal, que están transitando sus estudios en una institución pública o en uso de un servicio básico del Estado, entre otras cosas.

Los derechos de esas y de todas las personas están garantizados por marcos de derechos humanos internacionales y por la legislación local, que establecen obligaciones y límites para el Estado en el tratamiento de datos, obligaciones y límites que a su vez varían según si esos datos entran en categorías como las de datos personales o datos públicos, como también varían las condiciones para el uso equitativo para la provisión de recursos y servicios. De esta manera, el presente artículo busca, a partir de la evidencia obtenida durante el transcurso del trabajo sobre *Inteligencia Artificial e Inclusión*, analizar efectivamente cómo el Estado utiliza este tipo de tecnologías en el ejercicio de sus funciones de cara a la ciudadanía.

Como marco general de análisis, es necesario considerar que la producción de los datos que procesan y analizan las tecnologías basadas en IA no es un proceso neutral. Como resalta Buschmann (2021, 41), en su análisis sobre el Sistema Predictivo del Delito Urbano implementado en Chile, cada dato implica una cadena social de producción que puede incorporar sesgos y perspectivas del contexto. Esto se traduce en que las bases de datos pueden estar conformadas por datos que registran situaciones irregulares o inexactas, lo que puede resultar en un sistema sesgado que reproduce prácticas discriminatorias.

De esta manera, para conocer el potencial impacto en derechos fundamentales no basta con analizar la tecnología en sí, esto es, examinar los algoritmos o los procesos

de automatización implementados, dado que ellos no se implementan de forma aislada o en un vacío. Las políticas que utilizan IA como instrumento se dan en contextos sociales y políticos específicos, en países con diversa composición demográfica, marcos normativos particulares, características democráticas atadas a procesos históricos y gestiones gubernamentales que responden a la coyuntura puntual de cada territorio. De esta manera, uno de los puntos centrales de este documento, radica en comprender cómo se articula una respuesta a una problemática pública dentro de red sociotécnica, que involucra tanto a agentes humanos como no-humanos, en un contexto histórico e institucional determinado (Velasco y Venturini, 2021, p. 11).

Siguiendo estas premisas como base, el artículo se divide en tres partes. Primero, una síntesis de los marcos normativos aplicables para garantizar los derechos fundamentales de las personas, en el marco del uso de tecnologías basadas en inteligencia artificial por parte del Estado. Luego, una descripción de los diez casos de uso analizados en el proyecto Inteligencia Artificial e Inclusión. Por último, un análisis de las formas en que estos usos representan riesgos para los derechos humanos, en función de la normativa y de las características propias de estos usos.

II. METODOLOGÍA PARA EL ANÁLISIS DE LA IMPLEMENTACIÓN DE LA INTELIGENCIA ARTIFICIAL

Como fue mencionado, dado el carácter sociotécnico del desarrollo y despliegue de estas tecnologías, para comprender sus potenciales impactos en los derechos, es necesario conocer su contexto de implementación, sobre qué población busca operar, cuál es el marco normativo aplicable a esa jurisdicción, qué prácticas de uso de datos se desarrollan en esos gobiernos, entre otras aristas contextuales. En este sentido, los diez estudios de caso han sido analizados con una metodología multidimensional, que pretende dar cuenta de esta multiplicidad de factores intervinientes en el potencial impacto en los derechos de las personas.

Esta metodología, desarrollada por Derechos Digitales para este proyecto, consta de cinco dimensiones:

1. Contexto nacional de implementación: busca comprender las características sociodemográficas y tecnológicas del país donde se implementan sistemas de inteligencia artificial. Se evalúan factores como la distribución de la población, el acceso a tecnologías, y las condiciones socioeconómicas que influyen en la efectividad del uso de IA por parte del Estado.

2. Contexto regulatorio e institucional: examina el marco legal e institucional que regula el uso de la IA en el ámbito estatal. Incluye la existencia de leyes, normas, instituciones especializadas y mecanismos de supervisión diseñados para garantizar el desarrollo y uso de la tecnología con respeto de derechos.

3. Infraestructura de datos: analiza los recursos tecnológicos y de datos que sustentan los sistemas de IA estatales, como la calidad de los conjuntos de datos, su interoperabilidad y la existencia de mecanismos para proteger la privacidad y la seguridad de la información. Uno de los puntos de interés está enfocado en las características de esos datos, principalmente respecto a la existencia de datos personales en las bases a ser analizadas y procesadas.

4. Proceso de la toma de decisión: explora cómo se integran los sistemas de IA en los procesos de toma de decisión estatal, considerando la participación de actores humanos, la transparencia de los criterios utilizados y las vías de rendición de cuentas.

5. Diseño tecnológico: se enfoca en las características técnicas y funcionales de los sistemas de IA implementados por el Estado, incluyendo sus objetivos, capacidades y posibles sesgos en su desarrollo. Esta dimensión busca analizar si los sistemas implementados cuentan con un diseño alineado con las necesidades y objetivos de la política pública.

Los estudios han sido desarrollados por investigadoras de cada país donde los casos tienen lugar, quienes trabajaron variablemente de forma individual o en equipo, y en representación de una organización o sin afiliación institucional. Las investigadoras vienen de espacios de formación académica, de la sociedad civil e incluso del activismo. Esta diversidad muestra la pluralidad de personas interesadas e involucradas en la agenda que impulsa un uso de tecnologías más democrático y en respeto de los derechos humanos.

Si bien las miradas surgen de puntos de vista diversos, los problemas a la hora de implementar esta metodología fueron comunes a todas las investigaciones. El primero de ellos fue la falta de información disponible para acceder a los casos. Una primera instancia para la selección de los estudios a realizar consistió en el desarrollo de un mapeo, por parte del equipo de Derechos Digitales, a partir de la búsqueda en fuentes abiertas de casos de uso en la región latinoamericana. Se utilizaron motores de búsqueda en la web abierta, se realizó búsqueda en publicaciones específicas de distintas entidades gubernamentales, y se hizo revisión de informes especializados de organismos internacionales y programas de financiamiento de uso de IA en el Estado,

entre otros métodos. La información encontrada fue, en la mayoría de los casos, incompleta y fragmentaria, presentando un desafío inicial dada la dependencia de la información provista por las fuentes oficiales de distintos gobiernos.

De esta manera, el segundo inconveniente surge de las dificultades a la hora de acceder a información de fuentes oficiales. Las investigadoras encontraron en los pedidos de acceso a la información un recurso fundamental para poder analizar las dimensiones 3, 4 y 5. Sin embargo, las respuestas a los pedidos muchas veces fueron incompletas o se demoraron, dificultando el desarrollo de las investigaciones. Además, algunos de los representantes gubernamentales se mostraron reticentes a participar de la investigación como fuentes oficiales.

El último inconveniente para mencionar surge del carácter efímero de algunas de las políticas encontradas. Durante la etapa de mapeo, fueron detectadas múltiples políticas que utilizaban o decían utilizar IA como instrumento central. Sin embargo, a la hora de buscar más información fue advertido que muchas de ellas fueron discontinuadas o interrumpidas, en principio por dos motivos. El primero, es la falta de financiamiento luego de una etapa piloto. El segundo, el resultado de algunos de los cambios de gestión de gobierno que tuvieron lugar durante los últimos años, con cambios en los esquemas de gestión y prioridades gubernamentales.

1. MARCOS NORMATIVOS APLICABLES

La implementación de tecnologías basadas en inteligencia artificial por parte del Estado plantea importantes desafíos en términos de protección de derechos fundamentales, lo que hace imprescindible referir a los marcos normativos aplicables. Esta sección aborda, en primer lugar, las obligaciones que surgen de los tratados internacionales de derechos humanos, como la Convención Americana sobre Derechos Humanos y el Protocolo de San Salvador, y su relación con los principios de legalidad, necesidad y proporcionalidad en el uso de IA. Además, se examina la normativa específica sobre protección de datos personales y acceso a la información en distintos países de la región, destacando avances, carencias y su intersección con proyectos de regulación sobre IA. El objetivo es ofrecer un panorama integral de las obligaciones legales y regulatorias que los Estados deben cumplir para garantizar la protección de derechos frente al creciente uso de estas tecnologías.

Los tratados internacionales de Derechos Humanos

Como fue mencionado al inicio, una de las preguntas que busca responder el proyecto *Inteligencia Artificial e Inclusión* es la relativa a en qué medida consideran los estados los criterios de legalidad, necesidad y proporcionalidad a la hora de implementar este tipo de políticas. Esta pregunta busca entender cómo los estados garantizan las disposiciones establecidas por los estándares del sistema interamericano de Derechos Humanos, puntualmente, las obligaciones derivadas de la Convención Americana sobre Derechos Humanos (CADH), el Protocolo Adicional a la Convención Americana sobre Derechos Humanos en materia de derechos Económicos, Sociales y Culturales (Protocolo de San Salvador) y los fallos de la Corte Interamericana de Derechos Humanos.

Los impactos en los derechos humanos relacionados con el uso de la inteligencia artificial ya han sido reconocidos en diversas resoluciones a nivel internacional. La reciente Resolución A/HRC/RES/48/4 del Consejo de Derechos Humanos de la ONU sobre el derecho a la privacidad en la era digital ha delineado algunos de los riesgos que implica la adopción de la inteligencia artificial para el ejercicio de los derechos humanos, los cuales ocurren "principalmente cuando [la IA] se emplea para identificación, seguimiento, elaboración de perfiles, reconocimiento facial, predicción de comportamiento y para establecer puntuaciones de individuos". La resolución establece que los Estados deben respetar los derechos humanos en la implementación de estos sistemas y adoptar medidas preventivas y recursos efectivos frente a violaciones y abusos del derecho a la privacidad, especialmente en el caso de mujeres, niños y personas en condiciones de vulnerabilidad.

Así, las obligaciones establecidas por los tratados internacionales son precisas respecto a los deberes que competen a los Estados al incorporar tecnologías basadas en IA. Para sintetizar dichas obligaciones, utilizaremos el análisis realizado por Alimonti y de Alcântara (2024), que ofrece una perspectiva clara en un informe reciente publicado por la organización Electronic Frontier Foundation, donde resaltan cuáles son los deberes que competen a los estados a la hora de incorporar tecnologías basadas en IA. Estas son algunas de las implicancias mencionadas por las autoras:

- **Protección de Derechos Humanos:** Los Estados deben garantizar que el uso de sistemas de IA no infrinja los derechos humanos, en cumplimiento de la CADH. Además, la formulación de políticas que incorporen IA debe seguir un enfoque de derechos humanos, guiado por los principios de la CADH y el Protocolo de San Salvador (artículo 2).

- **Participación Social y Transparencia:** Es esencial que los procesos de toma de decisiones que involucren IA sean transparentes y permitan la participación significativa, en línea con el derecho a la información y la participación consagrado en la CADH.

- **Evaluación previa de impacto en DDHH:** Antes de adoptar un sistema de IA, los Estados deben realizar una evaluación exhaustiva que considere su idoneidad, en cumplimiento de las obligaciones establecidas en la CADH y el Protocolo de San Salvador. Asimismo, el informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos resalta la necesidad de garantizar que estas herramientas cumplan plenamente con el derecho internacional de los derechos humanos, recomendando una moratoria, e incluso la prohibición, de aquellas tecnologías que no puedan ser utilizadas de manera compatible con estos estándares (OHCHR, 2021). Por otro lado, los Estados deben establecer mecanismos adecuados para supervisar el uso de IA en el sector público, en consonancia con el deber de rendición de cuentas establecido en la CADH.

- **Protección de grupos en situación de vulnerabilidad:** Se debe prestar especial atención al impacto diferenciado que el uso de IA puede tener sobre grupos históricamente discriminados, en cumplimiento de los principios de igualdad y no discriminación de la CADH.

- **Garantías para asegurar el principio de no discriminación:** Las políticas que utilizan IA deben estar diseñadas para prevenir la discriminación, en línea con el artículo 1.1 de la CADH, que establece la obligación de respetar y garantizar los derechos.

Por último, dado el peso de las iniciativas desarrolladas por el sector privado en la agenda de la IA, es importante resaltar que, aunque las herramientas de IA sean desarrolladas por entidades privadas, los Estados siguen siendo responsables por que su uso respete las obligaciones mencionadas, conforme a las obligaciones derivadas de la CADH y el Protocolo de San Salvador. Esta responsabilidad estatal se extiende no solo al uso directo de estas herramientas, sino también a al contenido de las contrataciones, licencias o cualquier tipo de formalización con las empresas proveedoras. En este sentido, los Estados deben asegurarse de que los datos recolectados, almacenados y procesados en estos sistemas cumplan con estándares de protección y seguridad adecuados.

Por su parte, las empresas privadas, como actores clave en el desarrollo y despliegue de estas tecnologías, tienen responsabilidades específicas en la protección de los

derechos humanos. Según los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas, las empresas deben identificar, prevenir, mitigar y, cuando sea necesario, remediar los impactos negativos que sus operaciones puedan tener en los derechos humanos, actuando de manera responsable en todas las etapas del ciclo de vida de sus herramientas de IA (OHCHR, 2011).

Esta síntesis busca resaltar la existencia de un marco normativo internacional que ampara a la ciudadanía frente a potenciales usos perjudiciales de tecnología. Estos marcos internacionales, que tienen carácter obligatorio para los Estados, son particularmente relevantes frente a otros instrumentos internacionales, que en el ámbito de la IA cobran particular relevancia. Hacemos referencia aquí a recomendaciones y principios éticos sobre IA, que, si bien pueden dar un marco de acción, no representan por sí solos fuentes de deberes vinculantes para los Estados.

Protección de Datos Personales y Acceso a la Información

En cumplimiento de los marcos internacionales de derechos humanos, cada país debe desarrollar normativas específicas que protejan los derechos de los ciudadanos, en cumplimiento de las obligaciones internacionales asumidas. Esto incluye incorporar los derechos y obligaciones reconocidos en tratados internacionales a la legislación interna de forma clara y efectiva. Asimismo, es fundamental que las normativas nacionales, como las leyes de Protección de Datos Personales (PDP) y de Acceso a la Información Pública, sean coherentes con las disposiciones internacionales, garantizando un marco de protección alineado con los estándares de derechos humanos. En este sentido, aunque la situación en la región es disímil y en evolución, estos marcos representan un punto de partida, más que un objetivo final, para asegurar la protección de derechos fundamentales.

En Chile, hasta hace poco tiempo, la legislación de PDP estaba enmarcada en la ley sobre Protección de la Vida Privada, promulgada en 1999 como Ley Nº 19.628, y que regulaba el tratamiento de datos de carácter personal en registros o bancos de datos. A pesar de ser una de las primeras leyes de protección de datos en Latinoamérica, como señala Valderrama (2021), fue objeto de críticas por su rápida desactualización y su ineficacia para proteger adecuadamente a las personas de un mal tratamiento de sus datos por terceros. Sin embargo, el Congreso de Chile, en agosto de 2024, aprobó un nuevo articulado para la Ley de Protección de Datos Personales, que da un marco específico a su tratamiento y crea la Agencia de Protección de Datos Personales. Esto representa un avance respecto de la situación regulatoria analizada en los casos, años atrás.

Por otro lado, Brasil también cuenta con una normativa reciente. La Ley General de Protección de Datos (LGPD), promulgada en 2018 y en vigor desde 2020, establece un marco legal para la protección de datos personales, con importantes similitudes con el RGPD de la Unión Europea, al igual que la nueva legislación chilena. Como analizan Cardoso et al. (2021), aplica a cualquier tratamiento de datos personales realizado en Brasil y define estos datos como información relacionada con personas identificadas o identificables, incluyendo datos sensibles. La ley creó la Autoridad Nacional de Protección de Datos (ANPD), encargada de supervisar el cumplimiento de la ley y aplicar sanciones por incumplimiento.

Así como Chile y Brasil cuentan con normativa reciente[2], la Argentina cuenta con un proyecto de ley[3] generado por la Agencia de Acceso a la Información Pública con la participación de empresas, instituciones públicas, organismos de la sociedad civil y la academia. El propósito de su creación fue actualizar la normativa vigente, la Ley Nº 25.326, sancionada en el año 2000, casi un cuarto de siglo atrás. Sin embargo, el proyecto de ley permanece en comisiones desde agosto de 2023, sin previsión de debate en sesiones plenarias.

Por otro lado, en el otro extremo de la escala, como afirman Sequera y Cuevas (2024), Paraguay no cuenta con una ley de protección de datos personales. El principal marco aplicable es la Ley 6534/2020, que se refiere específicamente a la protección de datos personales crediticios, pero no abarca de manera integral la protección de datos personales en general. Cabe resaltar el rol de la Coalición por la Protección de Datos Personales, en Paraguay, un grupo que ha estado trabajando activamente desde 2016 para promover la creación de un marco legal integral que regule el tratamiento de datos personales en el país. En 2021, esta coalición elaboró un borrador de propuesta legislativa, que aún no ha sido tratado en el parlamento, aunque, durante 2023, la propuesta estuvo incluida en el orden del día de la Cámara de Diputados en cuatro sesiones distintas (TEDIC, 2024).

De esta manera, como podemos ver, la situación de la protección de datos personales en la región no es homogénea. Esto es relevante a la hora de considerar la complementariedad de esta normativa con algunos proyectos de regulación específica

2 A la fecha de conclusión del presente informe, la nueva ley chilena está a punto de promulgarse y, con eso, comienzan dos años de vacancia desde su publicación antes de estar plenamente vigente.

3 Para más información: https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales

de la IA, en discusión en la actualidad en distintos países de la región. Es el caso, por ejemplo, de los proyectos en discusión en Chile y Brasil, que incorporan un esquema de riesgos similar al que posee la Ley de IA sancionada por el Parlamento Europeo. Cabe mencionar, como referencia, que dicha normativa, que funciona complementariamente con el RGPD, catalogaría como "sistemas de alto riesgo" a algunos de los casos analizados, dado que en esta categoría caen, por ejemplo, los sistemas automatizados para acceder a beneficios provistos por el estado, los utilizados para la gestión de políticas de empleo, gestión de políticas de seguridad y de administración de justicia[4].

Por otro lado, como fue mencionado en el apartado metodológico, la investigación visibiliza la necesidad de mejorar las prácticas de acceso a la información por parte de los gobiernos de la región, en lo respectivo al uso de IA y las características del uso para el desarrollo de sus funciones, sea esta información brindada de forma proactiva o bien de forma pasiva, esto es, a partir de una solicitud formalmente cursada.

La normativa relativa al acceso a la información pública en países como Chile, Argentina, Uruguay y México contempla un marco para ambos casos de acceso a información pública. Aunque no existen marcos específicos para regular la provisión de información que se refiera puntualmente a cuestiones sobre inteligencia artificial, en principio ello no debería ser necesario como marco diferenciado, ya que los Estados están obligados a garantizar la divulgación de esta información a partir de las normas generales de transparencia y acceso a la información pública. Por el contrario, es la aplicación de esos marcos la que admite revisión para facilitar la transparencia pública en materia de implementación de IA.

2. USOS DE INTELIGENCIA ARTIFICIAL EN EL ESTADO

En este apartado, analizaremos cómo los distintos Estados de la región utilizan tecnologías basadas en IA como instrumento para la implementación de políticas públicas, en virtud a la evidencia generada en el área de trabajo *Inteligencia Artificial e Inclusión*, como fuera mencionado. Esta línea programática tiene, como aspecto central, interés en el potencial impacto en los derechos humanos que tiene el uso de IA por parte del Estado. En concreto, busca responder a la pregunta: ¿cómo están implementando los gobiernos de América Latina la inteligencia artificial y cuáles son sus impactos en el desarrollo, la inclusión y los derechos humanos? Y, además, ¿cómo consideran los criterios de legalidad, necesidad y proporcionalidad?

4 Ley de IA del Parlamento Europeo, Anexo 3. Disponible en https://artificialintelligenceact.eu/annex/3/

Los casos analizados muestran ejemplos de uso en ámbitos sensibles de la administración pública, como las áreas de empleo, protección social, seguridad pública, educación y gestión de trámites, además de usos en la administración de justicia. Brindaremos detalles sobre cada uno de ellos. Cada caso, junto con su descripción, contará con recuadros explicativos sobre las características técnicas de las tecnologías utilizadas o de las bases de datos o empresas tecnológicas involucradas, siempre que sea pertinente y aporte a la comprensión.

Imagen 1. Distribución regional de los casos analizados

EMPLEO

En temas de empleo, los casos analizados fueron dos. Por un lado, la incorporación de IA en el marco del Sistema Nacional de Empleo (SiNE) en Brasil, una política laboral activa desde 1975. Por otro, la automatización de procesos en el marco del programa EmpleaPY, gestionado por el Ministerio de Trabajo, Empleo y Seguridad Social (MTESS) de Paraguay. En ambos casos, se trata de políticas de intermediación laboral, donde el objetivo es facilitar la conexión entre las personas que buscan empleo y las empresas u organizaciones que necesitan contratar trabajadores.

Dataprev, Empresa de Tecnología e Información de la Seguridad Social de Brasil, fue creada por la Ley 6.125, en 1974. Es una empresa pública vinculada al Ministerio de Economía, responsable de la gestión de la Base de Datos Sociales Brasileña. Proporciona herramientas tecnológicas para la implementación de políticas sociales del Estado brasileño.

En 2019, el **Sistema Nacional de Empleo** experimentó una transformación significativa con la introducción del "Nuevo SINE". Este proceso de reestructuración buscó modernizar el sistema a partir de la implementación de herramientas tecnológicas, como la IA para el análisis de correspondencia entre quienes buscan y ofrecen empleo, el uso y la importancia de los datos digitales con información del mercado laboral y la asociación con el sector privado (Bruno et al. 2021, p. 10).

Puntualmente, la implementación de herramientas de IA está enmarcada en el Plan de Transformación Digital del SINE, iniciado en 2019 por la Secretaría de Políticas Públicas para el Empleo (SPPE), a raíz del Nuevo SINE y, sobre todo, a la relación más amplia entre el Gobierno Federal brasileño y Microsoft (Bruno et. al. 2021, p. 14). El proyecto contempla el uso de herramientas de inteligencia artificial provistas por Microsoft al gobierno brasileño para los sectores de empleo y sustentabilidad. La oferta de Microsoft para el sector del empleo implica la implementación de IA para la intermediación de mano de obra en el Portal de Vacantes *(Portal de Vagas)* del SINE, el Portal Emplea Brasil, y la cualificación de los trabajadores a través de la Escuela del Trabajador 4.0, una plataforma de enseñanza a distancia desarrollada por la Secretaría Especial de Productividad, Empleo y Competitividad del Ministerio de Economía (SEPEC/ME) en asociación con la Agencia Brasileña de Desarrollo Industrial (ABDI), que incluye cursos de Microsoft a través de la herramienta de capacitación Microsoft Community Training (Bruno et. al. 2021, p. 14).

Además, la empresa estatal Dataprev, a través de su infraestructura tecnológica permite que las empresas privadas accedan a datos anonimizados de trabajadores registrados en el SINE. Esto se da en el marco del proyecto SINE Abierto, parte del proceso de modernización mencionado, que tiene por objetivo habilitar el acceso a la base de datos de trabajadores registrados en el SINE a empresas privadas y otras instituciones que operan en el segmento de intermediación laboral (Bruno et al., 2021,12).

El vínculo entre Microsoft y el Gobierno de Brasil se da a partir de un Acuerdo de Cooperación Técnica. Según afirman las investigadoras, la herramienta se sustentará en el uso de datos, tecnología digital e inteligencia artificial, apoyadas en las herramientas y licencias de Microsoft Dynamics, PowerBI Premium y herramientas de inteligencia artificial de la nube Azure. El plan de trabajo señala que la herramienta tecnológica utilizará el módulo Customer Insights de Microsoft Dynamics 365 para la unificación y el procesamiento de datos, siendo el resultado esperado la mejor comprensión sobre los trabajadores y vacantes. (Bruno et. al. 2021, p. 49).

Tanto el SINE como Emplea Py utilizan técnicas de Matching Semántico para encontrar correspondencia entre quienes ofrecen y buscan trabajo. Se trata de una técnica informática para identificar información relacionada semánticamente. Dadas dos estructuras de tipo gráfico, por ejemplo, clasificaciones, bases de datos de taxonomías o esquemas XML y ontologías, la correspondencia es un operador que identifica aquellos nodos en las dos estructuras que se corresponden semánticamente entre sí.

De igual manera, el caso **EmpleaPy**, en Paraguay, busca automatizar procesos para conectar empleadores y candidatos. La versión inicial, conocida como ParaEmpleo, fue creada por la empresa suiza Janzz Technology. Posteriormente, el Ministerio de Trabajo, Empleo y Seguridad Social (MTESS) generó una nueva versión, EmpleaPy, que busca incorporar toma de decisiones automatizada. Esta es la versión que se encuentra vigente al momento del estudio (Sequera y Cuevas, 2024).

En lo que respecta a la actualización y mejoras del software por parte del MTESS al software de la empresa Janzz Technology, las autoras de la investigación constataron, en una entrevista con el área técnica del Ministerio, que la nueva versión fue desarrollada internamente, desde cero, con financiación estatal (Sequera & Cuevas, 2024, p. 16). Esta versión reutilizó la forma que procesaba los datos la empresa Janzz Technology que lo hacía genéricamente, y se ajustó a sus necesidades específicas y nuevas funcionalidades.

A su vez, fuentes del área técnica consultadas por las investigadoras afirmaron que la plataforma EmpleaPy aún no utiliza Inteligencia Artificial. En su lugar, cuentan con un procesamiento complejo y automatizado de ciertos procesos algorítmicos, lo cual facilita la gestión de identificación de la persona, el legajo del perfil tanto de las personas como de las empresas, para luego agruparlos y sugerirles con las palabras claves y comunes que ambos utilizan. Incluso, aseguran que el proceso de agrupamiento lo hacen de forma manual. Lo único automático es la consulta y validación del perfil de la persona usuaria (Sequera y Cuevas, 2024, p. 16).

PROTECCIÓN SOCIAL

Sobre esta área de competencia de la función pública, fueron analizados tres casos: El programa "Auxilio de emergencia" en Brasil, la aplicación "Coronavirus UY", en Uruguay y por último, el Sistema "Alerta Niñez", en Chile.

El CadÚnico, creado en 2001, es una base de datos de identificación y caracterización socioeconómica de las familias brasileñas de bajos ingresos. Es utilizado para más de treinta políticas públicas en Brasil, siendo el principal instrumento la selección de familias de bajos ingresos para programas componentes de la Asistencia Social Federal.

El **Auxilio de Emergencia** (AE) es una política de transferencia de renta, cuyo objetivo es apaciguar los efectos económicos y sociales de la pandemia de COVID-19, y permitir a la población que se encuentra en situación de vulnerabilidad la permanencia del acceso a bienes de consumo, sobre todo alimentación (Tavares et al., 2022).

El Auxilio de Emergencia fue concedido automáticamente tanto a las personas beneficiarias del Programa Bolsa Familia[5], como a las personas registradas en la base de datos CadÚnico, si cumplían los criterios de elegibilidad del programa. En relación a las políticas públicas ya constituidas en el país, el AE se aprovechó de la estructura preexistente de los programas de transferencia de renta, como el Programa Bolsa Familia, pero para llegar a un nuevo público, que no

5 El Programa Bolsa Familia, implementado por el Gobierno Federal y activo desde 2003, es el mayor programa de transferencia de renta en Brasil. Además de aportar ingresos a familias en situación de pobreza, integra políticas públicas para ampliar el acceso a derechos básicos como salud, educación y asistencia social, articulando acciones complementarias en áreas como deporte, ciencia y trabajo para superar la pobreza. Para más información: https://www.gov.br/mds/pt-br/acoes-e-programas/bolsa-familia

era beneficiario de ninguna política social (el llamado público ExtraCad); además se implementaron nuevas medidas y tecnologías (Tavares et al., 2022, p. 14).

El Auxilio de Emergencia está compuesto por un intenso flujo de datos, que atraviesa todas las etapas del programa. La selección de personas beneficiarias es automatizada, realizada por la mencionada empresa Dataprev, que cruza múltiples bases de datos, de diferentes órganos del Gobierno, con los datos del CadÚnico y con los requerimientos para concesión del beneficio del público del ExtraCad, realizados por medio de la aplicación Auxilio de Emergencia (Tavares et al., 2022, p. 19).

El programa **Coronavirus UY**, administrado por el Ministerio de Salud Pública de Uruguay (MSP), funcionó como mecanismo de gestión de información para enfrentar la pandemia de COVID-19. Se trata de un sistema informático desarrollado a instancias de actores privados y públicos, principalmente por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (Agesic), que tiene una aplicación para teléfonos móviles como uno de sus más importantes componentes (Yael, 2021, p. 5).

Un Modelo Predictivo de Riesgo (PRM, Predictive Risk Model) es una herramienta que utiliza patrones establecidos en bases de datos para generar automáticamente una probabilidad (o un puntaje de riesgo) de que un evento específico le ocurra a un individuo en el futuro. Ya que los PRM suelen usar datos recopilados con otros fines (por ejemplo, bases de datos administrativas gubernamentales) y pueden ser automatizados, pueden examinar grandes poblaciones de manera eficiente para identificar un número reducido de personas que se encuentran en un riesgo elevado. (AUT & UAI, 2019, p. 107; citado en Valderrama, 2021).

La aplicación Coronavirus UY fue diseñada con el propósito de ofrecer información pública sobre estadísticas de contagio del entonces nuevo coronavirus y las medidas sanitarias vigentes en ese momento. También buscó monitorear posibles casos de infección mediante la recopilación de datos de autodiagnóstico, brindar asistencia médica remota durante los períodos de confinamiento y, a partir de mediados de 2020, alertar a los usuarios sobre posibles contactos con personas infectadas. El sistema centralizó la información para facilitar la planificación de acciones estatales, tanto a nivel general como en casos individuales, proporcionando desde recomendaciones de cuidado hasta atención médica a través de telemedicina (Yael, 2021, p. 5).

La base de datos utilizada por la aplicación Coronavirus UY, que centralizaba los formularios epidemiológicos, estaba bajo la administración del Ministerio de Salud Pública (MSP). Cada

prestador de salud gestionaba su propia base de datos de manera independiente. Los documentos clínicos electrónicos de los pacientes, actualizados por los médicos tratantes, se almacenaban en la institución médica donde el paciente había sido atendido. Toda la información generada por el personal de salud sobre un paciente específico debía mantenerse bajo custodia de la institución correspondiente. Además, los usuarios podían acceder a su historial médico a través de los portales web de los prestadores que ofrecieran esta opción o solicitándolo directamente con su cédula de identidad (Yael, 2021, p. 23).

Por último, el **Sistema Alerta Niñez** busca estimar y predecir el nivel de riesgo de los NNA de sufrir alguna vulneración en sus derechos, mediante un análisis de datos con diferentes modelos algorítmicos, para poder anticipar e intervenir de forma temprana y preventiva en cada caso. En la práctica, el sistema genera un *score* o "índice de riesgo" para cada NNA que permite clasificar los casos en orden de prioridad para las Oficinas Locales de Niñez. Junto con ello, el sistema se ha constituido en una plataforma de registro, gestión y monitoreo de los casos de NNA identificados con mayor riesgo (Valderrama, 2021, p. 23). Los modelos predictivos se entrenaron con datos provenientes de diversas fuentes, incluyendo SENAME, Chile Crece Contigo, el Ministerio de Educación (matrícula y rendimiento escolar en colegios públicos y privados), el Registro Social de Hogares, datos censales sobre vulnerabilidad barrial y estadísticas de delitos por barrios proporcionadas por la Subsecretaría de Prevención del Delito, considerando radios de 300 y 1.000 metros alrededor del hogar de cada NNA (Valderrama, 2021, p. 31).

Se trata de un sistema desarrollado y mantenido por la Subsecretaría de Evaluación Social e implementado para las Oficinas Locales de Niñez (OLN) de la Subsecretaría de la Niñez, ambas subsecretarías dependientes del Ministerio de Desarrollo Social y Familia de Chile. El rol de los modelos predictivos se reduce a la realización de una clasificación inicial según criterios de priorización para establecer un orden en el que se atenderán los casos. Tal puntaje de riesgo se muestra en una columna junto a otras columnas como las alertas territoriales y del Chile Crece Contigo. Si bien ya en el cálculo de las nóminas se restringe el universo de posibles NNA a atender, dependerá del coordinador y los gestores de casos de cada OLN si siguen o no el orden de prioridad estimado por el instrumento predictivo (Valderrama, 2021, p. 23).

SEGURIDAD PÚBLICA

En términos de seguridad pública, fue analizado un desarrollo del Centro de Análisis y Modelamiento en Seguridad (CEAMOS) de la Universidad de Chile junto

al Departamento de Análisis Criminal (DAC) de Carabineros de Chile, el **Sistema Predictivo del Delito Urbano**. Este desarrollo, implementado en cincuenta y ocho comisarías a lo largo del país, buscó predecir zonas de mayor riesgo de ocurrencia de delitos para dirigir el patrullaje policial preventivo en las ciudades, definiendo áreas de mayor vigilancia y control. Según indica el reporte, desde el Gobierno se entiende por vigilancia policial a las acciones tendientes "a evitar que se generen situaciones no deseadas o a detectarlas para su neutralización", con las correspondientes funciones operativas: "vigilancia preventiva, procedimientos policiales, fiscalización selectiva, servicios extraordinarios y cumplimiento de órdenes judiciales" (MDS, 2013, p. 10; citado en Buschmann, 2021, p. 22).

AUPOL (Automatización de Unidades Policiales) es la plataforma principal de carabineros para registrar y almacenar datos referentes a denuncias, detenciones, constancias e infracciones. Este sistema permite generar los partes policiales que se entregan a juzgados y fiscalías.

La tecnología utilizada en el contexto del Sistema Predictivo del Delito Urbano se basa en la predicción de delitos, que se define como cualquier sistema que analiza datos existentes para pronosticar eventos criminales (Buschmann, 2021, p. 9). Según afirma la autora, los sistemas de IA, en este contexto, utilizan técnicas de aprendizaje automático y análisis de datos, para identificar patrones en la ocurrencia delictiva. Estos patrones se basan en teorías criminológicas que sugieren que el crimen no se distribuye de manera aleatoria, sino que sigue patrones ambientales, situacionales y sociales que pueden ser analizados y comprendidos (Buschmann, 2021, p. 10).

El sistema de predicción de delitos utiliza dos tipos de datos. El primer tipo son los casos policiales, que incluye detenciones y denuncias relacionadas a delitos de mayor connotación social (DMCS) agrupados en las hipótesis de robo con fuerza y robo con violencia. Los casos son registrados por Carabineros en la plataforma AUPOL, incluyendo datos del funcionario que ingresa la denuncia o detención al sistema, y datos de identificación personal de los afectados, testigos, denunciantes y/o detenidos como nombre completo, número de rol único nacional o RUN, profesión, estudios, género, edad, características físicas, estatura y domicilio. El segundo tipo de datos considerados es la ubicación de servicios y atracciones urbanas identificadas como factores contextuales relevantes, que podrían motivar o facilitar la ocurrencia de un crimen. Sobre este último punto, según los desarrolladores del sistema, se considera la ubicación de bancos, paradas de buses, restaurantes y cajeros automáticos (Buschmann, 2021, p. 28). Estos datos se obtienen a través de información registrada

por carabineros en su sistema de información geográfico y de plataformas abiertas colaborativas como OpenStreetMap (Baloian et al., 2017; Carabineros de Chile, 2018; citado en Buschmann, 2021).

JUSTICIA

En cuanto al sector de la administración de justicia, fueron analizados dos casos, ambos en la República de Colombia. Se trata el primero del sistema PretorIA, implementado en la Corte Constitucional, y el segundo del Fiscal Watson, utilizado en el ámbito de la Fiscalía General de la Nación.

PretorIA utiliza técnicas de Procesamiento De Lenguaje Natural (PLN), que es un campo de la inteligencia artificial que se centra en la interacción entre las computadoras y el lenguaje humano. A través del PLN, el sistema puede analizar, categorizar y extraer información relevante de los textos de las sentencias de tutela. Esto incluye el etiquetado automático de documentos y la generación de estadísticas sobre los casos.

El sistema **PretorIA** utiliza procesamiento del lenguaje natural para apoyar el proceso de selección de tutelas en la Corte Constitucional de Colombia. Su función principal es clasificar y etiquetar sentencias de tutela según categorías previamente establecidas por personas expertas. El sistema trabaja con textos jurídicos en español y proporciona información sobre el contenido de las sentencias, así como datos estadísticos generales. En cuanto a su autonomía, PretorIA no tiene capacidad para tomar decisiones judiciales. Funciona como una herramienta de apoyo en el proceso de selección de tutelas, pero las decisiones finales son tomadas por los magistrados de la Corte Constitucional. El sistema no actúa de manera independiente y su función esperada es simplificar la labor en la revisión de casos. (Saavedra y Upegui, 2021, p. 5).

Las tutelas son acciones constitucionales establecidas en el artículo 86 de la Constitución Política de Colombia. Su propósito es la protección inmediata de los derechos fundamentales de las personas ante situaciones de vulneración o amenaza de vulneración. Este mecanismo permite a la ciudadanía solicitar la intervención de la Corte Constitucional o de jueces para salvaguardar sus derechos fundamentales de manera rápida y efectiva (Saavedra y Upegui, 2021, p. 18). PretorIA obtiene los datos de los expedientes de tutela que son remitidos por los jueces y tribunales de primera y segunda instancia a la Corte Constitucional. El sistema procesa textos de sentencias

y utiliza categorías definidas por el personal de la Corte para clasificar y etiquetar la información (Saavedra y Upegui, 2021, p. 46).

En Colombia, la Fiscalía General de la Nación ha implementado **Fiscal Watson**, una herramienta basada en inteligencia artificial desarrollada por IBM, para apoyar la gestión de información del **Sistema Penal Oral Acusatorio (SPOA)**. Este sistema centraliza información relacionada con investigaciones criminales, actuaciones judiciales y administración de elementos probatorios, entre otros. Fiscal Watson utiliza algoritmos avanzados para analizar datos estructurados y no estructurados, identificando patrones, tendencias y posibles conexiones entre casos judiciales, con el objetivo de facilitar la toma de decisiones de las funcionarias judiciales (Palacios et al., 2024, p. 11).

Fiscal Watson opera en la etapa de indagación de los procesos judiciales, momento en el cual busca y correlaciona información de investigaciones basándose en criterios predefinidos por las personas usuarias. Estos criterios pueden ser geográficos (ubicación del hecho) o cualitativos (detalles específicos del relato de los hechos). Por ejemplo, Watson puede detectar conexiones entre casos de homicidio que involucren un mismo victimario, patrones criminales similares en una región o coincidencias en modus operandi entre diferentes causas judiciales. Este análisis ayuda a los investigadores a obtener una visión más amplia y a identificar posibles vínculos que podrían no ser evidentes al revisar manualmente grandes volúmenes de datos (Palacios et al., 2024, p. 13).

El SPOA, principal fuente de información para Fiscal Watson, es un vasto sistema de información criminal que consolida datos de múltiples bases judiciales, policiales, administrativas, entre otras. Este sistema incluye módulos para registrar relatos de hechos, gestionar actuaciones judiciales, distribuir casos entre funcionarios y consultar expedientes. Uno de los módulos más relevantes para el funcionamiento de Watson es el que contiene los **relatos de los hechos**, es decir, las descripciones iniciales de los eventos registrados en los casos judiciales.

El papel del funcionario encargado de transcribir estos relatos es crítico, ya que cualquier omisión o error en los detalles puede llevar a resultados imprecisos, discriminatorios o incorrectos en el análisis realizado por Watson (Palacios et al., 2024, p. 14).

Para garantizar la seguridad e integridad de los datos, Fiscal Watson no accede directamente a la base de datos original del SPOA. En su lugar, utiliza una copia espejo del sistema, lo que asegura que la información original permanezca protegida mientras Watson realiza sus análisis y consultas (Palacios et al., 2024, p. 16).

EDUCACIÓN

La Secretaría de Educación del Estado de Guanajuato, en México, desarrolló el **Sistema de Alerta Temprana para la Prevención del Abandono Escolar (SATPE),** que busca reducir la tasa de abandono escolar en las escuelas de educación media. El sistema se enmarca dentro del Pacto Social por la Educación, una estrategia integral del gobierno de Guanajuato que busca mejorar la calidad educativa y garantizar la permanencia de estudiantes en el sistema escolar (Ricaurte y Nájera, 2024, p. 10). Este pacto se estructura en cuatro componentes principales: asegurar la asistencia escolar, garantizar que nadie se quede atrás en su aprendizaje, reconocer la figura docente, y fomentar la participación de las familias en el proceso educativo (Ricaurte y Nájera, 2024, p. 13).

Las herramientas de inteligencia empresarial (BI, por sus siglas en inglés) permiten generar tableros de análisis y visualización de datos utilizando interfaces de usuario intuitivas, facilitando su uso por personas sin conocimientos técnicos avanzados en procesamiento de datos.

Los datos utilizados por el Sistema de Actuación Temprana para la Permanencia Escolar (SATPE) provienen de varias fuentes, incluyendo el Sistema de Control Escolar, que recopila información sobre la matrícula, asistencia y rendimiento académico de los estudiantes en las escuelas públicas. También se utilizan datos del Catálogo de Escuelas Oficial del Estado de Guanajuato (CEO), que proporciona información sobre las escuelas en el estado, y de la Recopilación de Información para la Mejora de los Aprendizajes (RIMA), que se centra en indicadores de aprendizaje. Además, se considera información relacionada con la plantilla docente (Ricaurte y Nájera, 2024, p. 18). El manejo de datos sobre indicadores educativos y control escolar que se implementan para el SATPE se realiza a través del Software Power BI, un sistema de inteligencia empresarial desarrollado por Microsoft (Ricaurte y Nájera, 2024, p. 21).

Los datos utilizados fueron recolectados mediante el Aviso de Privacidad Simplificado de la Dirección de Servicios Escolares mediante el cual “se informa a los usuarios (madres y padres de familia, tutoras y tutores), las finalidades para las cuales se recaba la información de niñas, niños y adolescentes, obteniendo su consentimiento tácito y –en algunos casos–expreso” según lo indicado por la Unidad de Transparencia del Poder Ejecutivo del Estado de Guanajuato (Ricaurte y Nájera, 2024, p. 18).

GESTIÓN DE TRÁMITES Y SERVICIOS

Un chatbot es un programa informático diseñado para interactuar con los usuarios simulando una conversación humana a través de comandos de voz o texto, generalmente mediante internet. A lo largo de los años, los chatbots han evolucionado desde sus primeras versiones en los años 60 hasta convertirse en sistemas impulsados por algoritmos que les permiten aprender de las interacciones con los usuarios, optimizando así sus respuestas futuras. (Adamopoulou et al., 2020; citado en Ferreyra, 2024).

El último caso de estudio corresponde al Chatbot "Boti", implementado por el Gobierno de la Ciudad de Buenos Aires (GCBA). Se trata de un asistente virtual que permite a los ciudadanos interactuar y obtener información a través de WhatsApp. Este chatbot utiliza Procesamiento de Lenguaje Natural (PLN) y tiene un enfoque de dominio abierto, lo que le permite ofrecer respuestas sobre una amplia variedad de temas, incluyendo servicios gubernamentales, salud y movilidad urbana. Desde su lanzamiento, Boti ha evolucionado para incluir funciones como la asistencia durante la pandemia de COVID-19, brindando información sanitaria y permitiendo el acceso a servicios públicos, convirtiéndose en un canal de centralización de la comunicación entre la administración y la ciudadanía (Ferreyra, 2024, p. 10-12).

Según destaca el GCBA, Boti ha tenido un crecimiento significativo desde su implementación. Durante la pandemia de COVID-19 se convirtió en la principal fuente de información oficial sobre síntomas, prevención y gestión de turnos y certificados de vacunación, entre otras funcionalidades. Durante el primer trimestre de 2022, Boti llegó a su máximo histórico de 26 millones de interacciones mensuales convirtiéndose en el principal canal de comunicación de GCBA con la ciudadanía. Sin embargo, según afirma el autor en base a información oficial, posteriormente las cifras descendieron hasta ubicarse entre los 5 y los 2 millones de conversaciones por mes (Ferreyra, 2024, p. 6).

Este chatbot obtiene los datos de diversas fuentes y sistemas de gestión del Gobierno de la Ciudad. La información para las gestiones y trámites particulares se vincula con otros sistemas del Gobierno, como el Sistema de Trámites Digitales (STD) y la plataforma de Trámites a Distancia (TAD). Estos sistemas permiten que el área competente del gobierno atienda las solicitudes de los usuarios. Además, el GCBA asegura que los datos proporcionados por los usuarios están protegidos por acuerdos de confidencialidad y se utilizan únicamente para ejecutar las funcionalidades ofrecidas por el chatbot. En situaciones excepcionales, la información puede ser

conservada por un período extendido según lo considere la administración, siempre en cumplimiento, afirman, con la legislación de protección de datos (Ferreyra, 2024, p. 16).

3. ANÁLISIS Y DISCUSIÓN: PROBLEMÁTICAS ASOCIADAS AL USO Y PROCESAMIENTO AUTOMATIZADO DE DATOS POR PARTE DEL ESTADO COMO INSTRUMENTO DE POLÍTICAS PÚBLICAS

En esta sección analizaremos algunas de las implicancias de estos casos de uso, respecto de distintos riesgos para el ejercicio de derechos, en función de los datos con los que fueron entrenados, los que utiliza y los algoritmos con los que son procesados. Asimismo, las implicancias para la protección de datos personales y acceso a la información pública serán analizadas a la luz de la normativa de cada país analizado. Primero, es necesario profundizar en las implicancias de uno de los eventos más influyentes que tuvo lugar durante el desarrollo de esta investigación, la pandemia de COVID-19.

El rol de la pandemia: uso de tecnología para la gestión masiva de datos

Desde Derechos Digitales, en una investigación colectiva junto con el Consorcio AlSur, desarrollamos un estudio sobre las implicancias del uso de tecnología durante la pandemia (Consorcio AlSur, 2021). El estudio analizó las principales características de las aplicaciones móviles implementadas por los gobiernos en 14 países de la región y expresó una profunda preocupación por la falta de una perspectiva integral por parte de los Estados para garantizar el respeto a los derechos humanos, conforme a los estándares establecidos a nivel internacional. Este incumplimiento de sus obligaciones de protección ha llevado, en muchos casos, a la vulneración de dichos derechos (Consorcio Al Sur, 2021, p. 65).

La falta de acciones integrales por parte de los gobiernos para la protección de derechos genera preocupación no solo en el uso de aplicaciones móviles, sino también en relación con las tecnologías analizadas en el presente estudio. Dado que el programa *Inteligencia Artificial e Inclusión* inició en 2019, fue posible examinar el surgimiento de nuevas aplicaciones destinadas a gestionar aspectos relacionados con la pandemia en la región, así como la expansión del área de influencia de tecnologías o aplicaciones ya existentes. En cuatro de los diez casos analizados, la pandemia desempeñó un papel central en la implementación y crecimiento de estas tecnologías.

La aplicación CoronavirusUY, analizada por Yael (2021) es el ejemplo más claro y representativo de lo anterior. Como fue referido, se trata de una aplicación que tiene como función reunir información de manera centralizada para dirigir acciones estatales tanto a nivel general como respecto de casos individuales, donde tuvo la capacidad de proveer desde recomendaciones de cuidado hasta atención vía telemedicina (Yael, 2021, p. 5). Esta fue una de las iniciativas más destacadas dentro de una estrategia de implementación tecnológica que, además de la aplicación, incorporaba diversos servicios de atención a la ciudadanía a través de sitios web estatales y plataformas populares como Facebook y WhatsApp, presentados en forma de un asistente virtual (Yael, 2021, p. 7).

El segundo ejemplo corresponde al uso de inteligencia artificial en el marco del programa Auxilio de Emergencia en Brasil. En este caso, la tecnología se utilizó como una herramienta de gestión administrativa para implementar una política destinada a mitigar los perjuicios económicos y sociales causados por la pandemia. A diferencia de CoronavirusUY, el uso de IA fue interno y se limitó a la gestión administrativa. Aunque no participaron grandes empresas tecnológicas, la empresa estatal Dataprev desempeñó un rol central, como se mencionó anteriormente.

Por otro lado, la pandemia potenció el desarrollo de algunas implementaciones de IA ya existentes. El primer caso para mencionar, también en Brasil, es el del Sistema Nacional de Empleo (SINE). El acuerdo de cooperación técnica, que permitió la implementación de herramientas de inteligencia artificial, fue establecido en noviembre de 2020 entre el gobierno brasileño y Microsoft, y surge como respuesta de la empresa a una convocatoria pública de propuestas destinada a mitigar los impactos negativos de la pandemia de COVID-19 en el sector productivo de Brasil (Bruno et al., 2022, p. 6).

El último ejemplo para mencionar, que se vio ampliamente potenciado por la pandemia, es el chatbot Boti, implementado por el Gobierno de la Ciudad de Buenos Aires. Este chatbot tomó un rol preponderante, asumiendo funciones que van desde la gestión de trámites y turnos de vacunación, hasta la creación de una herramienta de autodiagnóstico que funcionaba mediante una red neuronal que podía clasificar sonidos de voz, respiración y tos, analizando audios de tos enviados por WhatsApp para detectar posibles casos sospechosos de COVID-19 (Ferreyra, 2024, p. 12). Durante su funcionamiento, en el marco de la pandemia, las interacciones mensuales de personas usuarias con el chatbot aumentaron de manera exponencial, pasando de algunos cientos de miles, a millones, con un pico de 26 millones durante principios de 2022 (Ferreyra, 2024, p. 6).

Esto resalta dos puntos clave que merecen atención. En primer lugar, el rol central de la inteligencia artificial en la implementación de políticas dirigidas a un gran número de personas usuarias, como en los cuatro casos mencionados. En segundo lugar, la relevancia de los acuerdos establecidos con grandes empresas tecnológicas para la provisión de estos servicios en tres de los casos, destacándose principalmente Meta (antes Facebook) y Microsoft. De los diez casos analizados, las tecnologías implementadas durante la pandemia son las que presentan una mayor dependencia de estas grandes empresas, incluyendo a Fiscal Watson, que depende completamente de los servicios de IBM.

Acceso a la información pública: desafíos entre la opacidad y la divulgación inadecuada de datos

Conforme fue mencionado en la introducción, uno de los puntos más problemáticos para la producción de información relativa a los estudios de caso fue el acceso a la información y fuentes de consulta que permitan analizar cómo el Estado usa estas tecnologías.

En el reporte sobre el Sistema Predictivo del Delito Urbano, Buschmann (2021, p.9) afirma que, si bien Carabineros ha incorporado espacios para fortalecer la transparencia y probidad administrativa, como el Departamento de Información Pública y Lobby, el Departamento de Reclamos y Sugerencias, y la plataforma de estadísticas criminales STOP; gran parte de los datos publicados no se encuentran desagregados, la distribución del personal policial en el territorio es secreta, y hay poca información relativa a faltas cometidas por personal de Carabineros. Además, afirma Buschmann, las investigaciones sumarias dentro de Carabineros tienen carácter secreto, lo que ha sido cuestionado por la Convención Interamericana de Derechos Humanos y se contrapone al principio de probidad establecido en la Constitución chilena. Por otro lado, la autora marca una problemática ligada al Consejo para la Transparencia. Afirma que su rol fiscalizador, como el de todo organismo público, está limitado al cumplimiento de normas y no a la resolución de problemas sobre solicitudes de información. Esto se relaciona, a su vez, con la necesidad de reconocer el acceso a la información pública como derecho fundamental consagrado en la Constitución (Castillo, 2009; CIDH, 2016; citados en Buschmann, 2021, p.9).

En su estudio sobre el chatbot Boti, Ferreyra (2024, p. 4) afirma que la recolección de información sobre las características de funcionamiento del chatbot, así como sus mecanismos de gestión interna, se basan en fuentes abiertas, y en un pedido de acceso a la información pública presentado ante el GCBA, “cuya vaguedad en buena

parte de las respuestas motivó una segunda solicitud que, al momento de finalizar la investigación, no había sido contestada" (Ferreyra 2024, p. 4). Cabe aclarar que la Ciudad de Buenos Aires cuenta con una ley de acceso a la información reformada recientemente (Ley 104, 2017), que fue resultado de un proceso abierto de consultas públicas. Sin embargo, la existencia de esta ley no ha sido garantía para el acceso efectivo a información sobre uso de tecnología por parte del GCBA. Otro ejemplo es el que tuvo como protagonista al Observatorio de Derecho Informático Argentino (O.D.I.A.), quien realizó dos pedidos de acceso a la información pública sobre el uso de IA en cámaras de reconocimiento facial en la Ciudad de Buenos Aires. Según fuentes del Observatorio, estos dos pedidos de acceso no fueron respondidos de manera satisfactoria, por lo que presentaron una acción de amparo para detener el Sistema de Reconocimiento Facial de Prófugos de la Ciudad de Buenos Aires. En una primera instancia la acción fue rechazada, pero luego apelaron y ampliaron la demanda para pedir por la inconstitucionalidad del uso de esta tecnología[6].

En contraste, en el caso del Auxilio de Emergencia, las investigadoras no analizan un problema de falta de información, sino la divulgación de datos personales, incluidos datos sensibles, de manera contraria a los principios de protección de datos y a los derechos de las personas. Las autoras (Tavares et al., 2022, p. 33) sostienen que cualquier acto de la administración pública en Brasil está obligado a observar el principio de transparencia, establecido originalmente en el mandato constitucional de cumplir con el principio de publicidad, positivado en el artículo 37. Los efectos de este principio en la gestión pública se consolidaron en 2011 con la promulgación de la Ley de Acceso a la Información (Ley 12.527/11), que estipula como directriz que la publicidad es la regla general y la confidencialidad, la excepción. En este marco, los actos y procedimientos relacionados con las Ayudas están sujetos a dichas obligaciones legales, y las autoridades competentes, en particular el Ministerio de la Ciudadanía y las empresas públicas Caja Económica y Dataprev, deben poner a disposición toda la información al respecto, sin necesidad de solicitudes previas, siempre que se confirme el interés público y se respeten los derechos fundamentales involucrados (Tavares et al., 2022, p. 33).

Sin embargo, las autoras destacan que, en contraste con la falta de transparencia activa en decisiones automatizadas sobre la gestión de datos, se observa un uso excesivo e indiscriminado de este principio en el ámbito político. Esto se evidenció con la publicación en el Portal de Transparencia de un listado con datos personales de las personas beneficiarias del programa, incluyendo nombre completo, montos y cuotas

6 Para más información, consultar la web oficial de O.D.I.A.: https://srfp.odia.legal/

recibidas, entre otros datos sensibles. Justificado por razones de rendición de cuentas y prevención de fraudes, este enfoque entra en conflicto tanto con la Ley de Acceso a la Información, que exige proteger los datos personales, como con los principios fundamentales de protección de datos (Tavares et al., 2022, p. 33). Este escenario evidencia una baja adecuación de las políticas de protección social a la cultura de protección de datos, así como una negligencia hacia la autodeterminación informativa, reconocida por el Supremo Tribunal Federal como un derecho fundamental, al impedir que las personas ejerzan control sobre sus datos personales en el programa (Tavares et al., 2022, p. 33).

Un último caso relevante para analizar es el del Sistema Alerta Niñez (SAN) de Chile. Según Valderrama (2021, p. 8), el informe se basó en información obtenida mediante una solicitud de acceso a la información amparada por la Ley de Transparencia, complementada con una revisión exhaustiva de documentación secundaria, como prensa, presentaciones, licitaciones, propuestas técnicas, orientaciones técnicas, informes, cuentas públicas y órdenes de compra del ministerio responsable y otras entidades. Sin embargo, el autor destaca las dificultades encontradas durante el proceso de investigación, entre ellas, la negativa explícita de actores clave del Ministerio de Desarrollo Social y Familia a participar en entrevistas, así como la falta de documentación pública actualizada sobre el estado del instrumento predictivo del SAN, que ya se encontraba en implementación en las Oficinas Locales de Niñez (Valderrama, 2021, p. 8).

Consideraciones sobre protección de datos personales

Dado que las tecnologías de IA estudiadas se fundamentan en el manejo de una cantidad masiva de datos, resulta esencial abordar las consideraciones sobre protección de datos personales identificadas por las personas investigadoras. Si bien en algunos casos la falta de cumplimiento de los criterios de protección de datos personales es evidente, en otros, aunque el Estado otorgue ciertas garantías, los estudios subrayan la necesidad de una supervisión rigurosa que garantice efectivamente la protección enunciada.

En Chile, el Sistema Alerta Niñez plantea preocupaciones específicas sobre el manejo de datos personales de niños, niñas y adolescentes (NNA), los cuales son considerados especialmente sensibles por el Consejo para la Transparencia (CPLT). Según el CPLT, los datos de NNA requieren una protección reforzada debido a la falta de consentimiento informado claro y a que estas personas pueden ser menos conscientes de los riesgos

del tratamiento de sus datos. Por ello, el Consejo ha limitado la entrega de información sobre menores a casos en los que se acredita ser el tutor legal. En otros casos, ha negado el acceso para evitar daños probables y específicos a la privacidad de los menores (Valderrama, 2021, pp. 14-15). El CPLT también ha cuestionado acuerdos como el convenio entre el Servicio Nacional de Menores y la Agencia Nacional de Inteligencia por no ajustarse a los estándares de protección de datos de NNA. Este posicionamiento se alinea con la Convención de los Derechos del Niño, que prohíbe injerencias arbitrarias en la vida privada de los menores, y con el principio del interés superior del niño, a partir del cual se puede considerar que los datos de menores tratados en el sistema educacional no deben considerarse como información de acceso público, según afirma una especialista consultada por el autor (Valderrama, 2021, pp. 14-15).

En Colombia, el sistema PretorIA, desarrollado por la Corte Constitucional, automatiza la selección de expedientes de tutela para revisión, sin procesar datos personales sensibles, según afirman los autores, Saavedra y Upegui (2021, p. 47). Este sistema opera sobre textos de sentencias judiciales y no introduce cambios en el acceso o tratamiento de datos personales, dado que el proceso tradicional ya requería remisión de documentos judiciales. La Corte ha asegurado que el funcionamiento del sistema no depende de nombres ni datos específicos, pudiendo operar con información anonimizada. Además, la Ley 1581 de 2012 establece excepciones al consentimiento en el tratamiento de datos necesarios para funciones judiciales. Sin embargo, aunque el sistema no introduce cambios en el acceso o tratamiento de datos personales, ni afecta directamente los derechos subjetivos, su impacto social es significativo. Este impacto radica en su rol dentro de un proceso judicial que requiere legitimidad y confianza pública. Por ello, los autores destacan la necesidad de una supervisión técnica y operativa rigurosa para evitar defectos en su funcionamiento y garantizar la transparencia y legitimidad del proceso (Saavedra y Upegui, 2021, p. 47)

En Uruguay, el sistema Coronavirus UY centralizó información personal de pacientes, como edad, teléfono, cédula de identidad, síntomas y enfermedades preexistentes. Esta información fue organizada en una base de datos única, accesible al Ministerio de Salud Pública (MSP) y a prestadores de salud, quienes la utilizaron para el seguimiento de pacientes. La base de datos centralizada estuvo bajo la propiedad del MSP y es esa entidad la encargada de establecer las pautas y protocolos de su uso (Yael, 2021, p. 17). Los datos personales utilizados por la aplicación están protegidos por la legislación local en materia de protección de datos personales (Ley Nº 18.331). Esta normativa establece los datos de salud como especialmente sensibles (Art. 4) y que, según los artículos 17 y 19, solo pueden ser tratados por establecimientos de salud y para el cumplimiento de los fines directamente relacionados con el interés legítimo del emisor

y del destinatario, con el previo consentimiento del titular de los datos. Sin embargo, el mismo día del lanzamiento de la aplicación, el 20 de marzo de 2020, la Unidad Reguladora y de Control de Datos Personales (URCDP) emitió un dictamen (Dictamen Nº 2/020) que estableció que, debido al estado de emergencia sanitaria y en razón de la habilitación legal, el tratamiento de los datos de salud, tales como los recolectados por la aplicación Coronavirus UY, puede realizarse sin previo consentimiento de los titulares de los datos. Por otro lado, el MSP cumple un rol de auditoría y contralor en el ecosistema de datos. Esto presenta un ejemplo de los usos excesivos de datos sensibles realizados por el estado durante la pandemia, con un riesgo muy alto para la vulneración de derechos.

Problemas sobre el uso automatizado de datos y algoritmos

Resulta pertinente analizar la potencial vulneración de derechos que puede derivarse de la construcción de tecnologías, particularmente en relación con los algoritmos o sistemas basados en IA, así como con los datos utilizados para su entrenamiento y procesamiento. Un ejemplo relevante para este análisis es el caso del Sistema Alerta Niñez, implementado en Chile.

Conforme afirma Valderrama (2021, p. 31), para modelar el algoritmo del Sistema Alerta Niñez, se utilizaron datos que provienen principalmente de personas que han interactuado con los servicios estatales de educación y asistencia social, las cuales tienden a tener menores ingresos o niveles educativos. Esto podría dar lugar a disparidades según el nivel socioeconómico, lo que implica que el modelo podría tener una menor capacidad para identificar a niños en situación de alto riesgo pertenecientes a niveles socioeconómicos más altos y, al mismo tiempo, podría aumentar el riesgo estimado para las familias de niveles socioeconómicos más bajos (Valderrama, 2021, p. 36). Por lo tanto, es crucial considerar la representatividad de los datos y buscar formas de incluir información más amplia y diversa para mejorar la precisión y equidad del sistema predictivo y, de esta manera, fortalecer el funcionamiento de la política pública en que se enmarca su funcionamiento.

Otro cuestionamiento lo podemos encontrar en el mencionado Auxilio de Emergencia, implementado por el Gobierno Federal de Brasil. Como fue mencionado, el caso analizado se basa en un uso intenso de datos para la selección automatizada de beneficiarios. Esta infraestructura de datos se basa en el cruce de 34 bases de datos diferentes, que incluyen registros del “Cadastro Único”, el Registro Nacional de Información Social (CNIS), y datos de diversas entidades gubernamentales, como el

Ministerio de Economía y la Caja Económica Federal. Sin embargo, esta complejidad enfrenta serias limitaciones debido a la obsolescencia de los registros (Tavares et al., 2022, p. 31). En particular, se ha identificado que bases de datos clave, como la Relación Anual de Información Social (RAIS), no se actualizan con información reciente, lo que impacta negativamente a aquellos que han perdido sus empleos o han experimentado cambios en su situación laboral desde el año base de 2018. Esta falta de actualización en los registros ha resultado en la exclusión de personas que, a pesar de cumplir con los criterios de elegibilidad, no pueden acceder al beneficio. Así, la arquitectura digital del programa, en lugar de facilitar la inclusión social, refuerza las barreras de acceso y limita la efectividad de la política de protección social. Como se analizará más adelante, esta situación derivó en la judicialización del programa, lo que permitió una evaluación detallada de su funcionamiento.

En relación con el Sistema Predictivo Urbano en Chile, es pertinente cuestionar los efectos de reforzar sesgos, no solo en términos de sobrevigilancia de determinados espacios o zonas, sino también respecto a cómo la implementación de tecnologías basadas en estos sesgos puede perpetuar prácticas discriminatorias al focalizar la vigilancia en áreas previamente catalogadas como conflictivas. Conforme relata Buschmann (2021, p. 41), el Sistema Predictivo del Delito Urbano se alimenta principalmente de dos fuentes de datos: los casos policiales, que incluyen detenciones y denuncias relacionadas con delitos de mayor connotación social (DMCS), y la información recopilada a través de la plataforma AUPOL, utilizada por Carabineros. Estos datos abarcan información personal de los afectados, testigos y denunciantes, como nombre, RUN, profesión, género y domicilio. Sin embargo, la producción de estos datos no es un proceso neutral. Según analiza Buschmann (2021, p. 41), cada dato implica una cadena social de producción que puede incorporar sesgos y perspectivas del contexto. Esto se traduce en que la base de datos puede estar conformada por datos que registran situaciones irregulares o inexactas, como detenciones arbitrarias o denuncias no investigadas, lo que puede resultar en un sistema sesgado que reproduce prácticas discriminatorias, especialmente en la aplicación de controles de identidad preventivos. En la investigación se evidenció la falta de protocolos de evaluación o auditoría externa en la recolección de datos (Buschmann, 2021, p. 7).

Contrapesos democráticos: el rol de los organismos de control y de la justicia

De esta manera, cabe preguntarse por el rol de los organismos de contralor que puedan equilibrar la balanza a favor de la protección de derechos, principalmente las defensorías públicas y las unidades de auditoría externa, como organismos oficiales

con funciones de control externo a la gestión gubernamental. Por otro lado, también analizaremos el rol que la justicia tuvo en algunos de los casos, como espacio de denuncia por parte de la ciudadanía para enmendar problemas vinculados a las fallas en las políticas analizadas, en parte, ocasionadas por un inadecuado procesamiento de datos.

El caso del uso de Boti, en la Ciudad de Buenos Aires, es un buen ejemplo en este sentido. Como relata Ferreyra en su estudio sobre el chatbot gubernamental (2024, p. 20), durante 2022, la Auditoría General de la Ciudad de Buenos Aires (AGCBA), organismo público de control externo, llevó a cabo un análisis exhaustivo de los sistemas, procesos y tecnologías que garantizan la operatividad del chatbot Boti, abarcando el año 2021. El informe de auditoría, publicado en marzo de 2023[7], reconoció el proceso de modernización llevado adelante por el Gobierno de la Ciudad para facilitar el acceso a información para la gestión de trámites y turnos, pero también áreas críticas que requieren mejoras, especialmente en la formalización de procedimientos administrativos relacionados con el chatbot. El dictamen de auditoría destacó la necesidad de establecer políticas informáticas robustas para la gestión y protección de datos personales, así como la importancia de una gobernanza efectiva en las tecnologías de la información y las comunicaciones. La auditoría subrayó que la gestión y almacenamiento de grandes volúmenes de información requieren una revisión constante de las políticas para garantizar la seguridad y protección de los datos procesados.

Sobre este mismo caso, podemos citar un ejemplo más. En 2022, la Defensoría del Pueblo de la Ciudad de Buenos Aires, autoridad de protección de datos personales de la Ciudad, realizó una investigación en respuesta a una denuncia sobre el funcionamiento del chatbot Boti (Ferreyra, 2024, p. 21). La denuncia, generada por una ciudadana, se basaba en su preocupación por la falta de disponibilidad del aviso legal al ingresar al asistente virtual Boti en la página web oficial del gobierno porteño, además de señalar que, a través de este chatbot, cualquier persona con conocimiento del DNI y número de teléfono de un tercero podía obtener información sensible, como los resultados de los tests de COVID-19. A partir de la constatación de estos hechos, la Defensoría emitió recomendaciones para mejorar la claridad y la integridad del aviso legal, así como para garantizar la adecuada inscripción de bases de datos en el registro correspondiente. Se enfatizó la necesidad de un manejo ético y seguro de los datos personales, destacando la importancia de cumplir con las normativas de protección de datos.

7 Disponible en: https://www.agcba.gov.ar/docs/inf-20230322_2202---CHATBOT-BOTI..pdf (consultado en noviembre 2024)

El sistema judicial desempeñó un papel crucial como intermediario entre la ciudadanía y el gobierno en la garantía del ejercicio de derechos. Ante los problemas señalados en el marco del Auxilio de Emergencia en Brasil, y debido a la ausencia de mecanismos administrativos para revisar las decisiones automatizadas, la vía judicial se convirtió en el principal recurso para cuestionar dichas decisiones y solicitar un análisis humano en la concesión del beneficio. Por tratarse de un programa federal, la contestación judicial tuvo lugar ante la Justicia Federal (Tavares et al., 2022, p. 37). La judicialización del Programa se intensificó debido a la desactualización de los registros en los sistemas del Gobierno Federal. Existen casos de personas desempleadas que, a pesar de no tener empleo formal, aparecían con un vínculo laboral vigente en las bases de datos, lo que les impidió acceder al beneficio. Esta situación llevó a un aumento significativo en el número de acciones judiciales de reclamación, alcanzando casi 76,000 en septiembre de 2020 (Tavares et al., 2022, p. 22). Para abordar esta problemática, se estableció un convenio entre la Defensoría Pública Federal y el Ministerio de la Ciudadanía, permitiendo a la Defensoría acceder a un sistema específico de Dataprev para la consulta y presentación de impugnaciones administrativas (Tavares et al., 2022, p. 22). De esta manera, según afirman las autoras, puede considerarse que la falta de revisión humana en las decisiones automatizadas ha perpetuado la judicialización, evidenciando las limitaciones del sistema para garantizar un acceso inclusivo al Auxilio de Emergencia (Tavares et al., 2022, p. 31).

Sobre este punto, Buschmann (2021, p. 9) analiza el rol de la Contraloría General de la República, una institución clave en Chile para la transparencia y el control público. Este órgano autónomo supervisa la inversión de fondos de diversas entidades estatales, incluidas las policías, objeto de su estudio. Durante los exámenes de rendición de cuentas, la Contraloría puede formular reparos y observaciones, verificando la legalidad de sus actos mediante auditorías que evalúan actividades, resultados y procedimientos para determinar si cumplen con las normas y principios establecidos. Según la autora, estas auditorías incluyen controles financieros, de legalidad, de gestión, de resultados, de revisión de cuentas y de evaluación del control interno. Este enfoque ha permitido identificar problemáticas relacionadas con las plataformas digitales utilizadas por Carabineros, las cuales fueron examinadas en el marco de su investigación (Buschmann, 2021, p. 9).

El rol de los organismos de control y contralor es un ejemplo significativo de cómo el Estado, en el marco de su funcionamiento democrático, puede mitigar las fallas identificadas en los apartados analizados en esta sección. Estos organismos han intervenido en casos de vulneraciones relacionadas con la protección de datos personales, el acceso a la información y los problemas derivados de bases de

datos desactualizadas y, en última instancia, inadecuadas para la automatización de procesos. Sin embargo, es fundamental destacar la importancia de realizar evaluaciones previas y garantizar que la implementación de estas tecnologías respete los marcos de derechos humanos, evitando así situaciones en las que los derechos ya hayan sido vulnerados antes de la intervención de los organismos de control.

CONCLUSIONES

En el marco del proyecto Inteligencia Artificial e Inclusión, en un período de casi seis años, fueron analizados diez casos de uso de tecnología en siete países de América Latina. Durante ese período, entre 2019 y 2024, el desarrollo de tecnologías basadas en IA aumentó notablemente, así como la difusión de su uso, principalmente a partir de la masificación del uso de IA generativa, a fines de 2022. También, durante este período, comenzó y finalizó la pandemia de COVID-19, lo que presentó una situación excepcional que intensificó el uso de tecnología como instrumento de gestión de trámites y servicios, pero también de políticas nodales para la protección social. Asimismo, durante este período tuvo lugar el lanzamiento de algunos de los marcos éticos y regulatorios más influyentes para la región, como los Principios de la OCDE para una IA Fiable (2019)[8], la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO (2021)[9] o la Ley de Inteligencia Artificial de la Unión Europea (2024)[10]. A continuación, analizaremos qué factores persisten y qué cambió respecto del uso de IA en el estado durante este período.

La primera observación tiene que ver con la persistencia en una falta de marcos normativos adecuados para la implementación de estas tecnologías. Sobre este punto son ilustrativos los datos del primer reporte del Índice Global de Inteligencia Artificial Responsable, publicado en 2024. Para las dimensiones de acciones y marcos de gobierno, basadas en el análisis de la existencia de estrategias nacionales de IA, evaluaciones de impacto en derechos, acciones para la revisión humana, consideraciones de proporcionalidad, pautas claras de transparencia y explicabilidad, entre otros, solo dos países de la región superaron el 50% del puntaje. Para la dimensión de Derechos Humanos e IA, ninguno de los países supera el 50% del puntaje.

8 Disponibles en: https://oecd.ai/en/ai-principles

9 Disponibles en: https://www.unesco.org/es/legal-affairs/recommendation-ethics-artificial-intelligence

10 Más información en https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Esta dimensión de análisis contempla indicadores sobre equidad de género, protección de datos y privacidad, participación pública, derechos de NNA, protección de trabajadores, entre otras[11]. Esta es una de las conclusiones que se refuerzan respecto del primer informe comparativo publicado en el marco de este proyecto (Velasco y Venturini, 2021), donde ya fue advertida la ausencia de marcos específicos para el uso de IA en el Estado.

En el ámbito de la protección y uso de datos personales, los organismos de control desempeñaron un papel crucial para evitar que el procesamiento automatizado de datos vulnerara derechos fundamentales, como el acceso a beneficios sociales. Un ejemplo particularmente ilustrativo es el caso del Auxilio de Emergencia en Brasil, donde las deficiencias en la actualización de las bases de datos causaron perjuicios significativos a las personas que intentaron acceder a este programa. Este caso evidencia los riesgos asociados a políticas basadas en el procesamiento automatizado de datos y subraya la importancia de garantizar la calidad de los datos que serán procesados por los algoritmos.

En cuanto al acceso a la información pública, se observa un problema persistente que atraviesa casos en todas las etapas de publicación. La respuesta incompleta a un pedido de acceso a la información, como ocurrió con el chatbot Boti en la Ciudad de Buenos Aires, o la negativa explícita a brindar entrevistas, como en el análisis del Sistema Alerta Niñez en Chile, son ejemplos que ilustran las dificultades para investigar el uso de inteligencia artificial por parte del Estado. Sin embargo, la falta de transparencia no es el único desafío; también lo es la publicación de información que no respeta la protección de los datos personales, como se evidenció en el caso del Auxilio de Emergencia en Brasil. En este caso, se publicó a través del Portal de Transparencia un listado con datos personales de las personas beneficiarias del programa. Aunque esta acción fue justificada bajo el argumento de rendición de cuentas, como señalan las autoras, entra en conflicto con la Ley de Acceso a la Información, que exige al poder público proteger los datos personales, y con los principios de protección de datos (Tavares et al., 2022, p. 33). Por lo tanto, es fundamental concebir e interpretar los marcos normativos de manera complementaria para garantizar que se priorice la protección de los derechos fundamentales de las personas.

Otro punto de alerta es la persistencia en la falta de espacios de participación significativa, que garantice espacios de diversidad e inclusión de las múltiples partes

11 El reporte completo está disponible en: https://www.global-index.ai/Region-South-and-Central-America

interesadas, no solo en el marco de implementación de políticas, impulsadas por los distintos poderes del Estado sino también en los incipientes espacios de regulación. En una investigación previa, desde Derechos Digitales analizamos los procesos participativos generados en el marco de los llamados planes y estrategias de inteligencia artificial impulsados por distintos gobiernos en la región. Esta investigación muestra que, si bien hubo esfuerzos por generar espacios participativos, los esfuerzos aún son insuficientes para dotar de empoderamiento a la ciudadanía en la toma de decisiones sobre políticas públicas que puedan afectar directamente el goce de sus derechos (Hernández et al. 2022).

De este modo, se evidencia la persistencia de problemáticas relacionadas con la protección de datos personales, el acceso a la información pública y la falta de espacios de participación significativa en la implementación de tecnologías de inteligencia artificial por parte del Estado. Si bien la adhesión a marcos éticos es conveniente, no es suficiente; resulta fundamental establecer reglas claras y marcos de gobernanza que garanticen la participación de múltiples partes interesadas. Desde Derechos Digitales, consideramos prioritaria la incorporación de una perspectiva de derechos humanos en todos los procesos relacionados con la regulación de la inteligencia artificial, ya sea a través de iniciativas del poder ejecutivo o de los parlamentos de la región, con el objetivo de promover un uso responsable e inclusivo de estas tecnologías en la gestión gubernamental; que incluya limitaciones claras para su uso.

BIBLIOGRAFÍA

Alimonti, V., & Cavalcanti de Alcântara, R. (2024). Estándares interamericanos y uso estatal de la IA en decisiones que afecten derechos humanos: Implicaciones para los DDHH y marco operativo. Electronic Frontier Foundation. https://www.eff.org/document/estandares-de-derechos-humanos-para-el-uso-estatal-de-la-ia-en-america-latina

Bruno, F., Cardoso, P. & Faltay, P. (2021). *Sistema Nacional de Empleo y la gestión automatizada de la desocupación laboral*. Derechos Digitales.

Buschmann, J. (2021). *Sistema predictivo del delito urbano: Producción algorítmica de zonas de vigilancia y control en la ciudad.* Derechos Digitales.

Consorcio Al Sur (2021) Informe Observatorio Covid-19: Un análisis crítico de las tecnologías desplegadas en América Latina contra la pandemia. Consorcio Al Sur. https://www.alsur.lat/reporte/informe-observatorio-covid-19-consorcio-al-sur-un-analisis-critico-tecnologias-desplegadas

Ferreyra, E. (2024). Boti: *estudio sobre el chatbot con procesamiento del lenguaje natural del Gobierno de la Ciudad de Buenos Aires*. Derechos Digitales.

Hernández, L., Canales, M.P. & Souza, M. (2022) I*nteligencia Artificial y participación en América Latina: Las estrategias nacionales de IA*. Derechos Digitales.

Nájera, J., Ricaurte, P. (2021). Tecnologías de interés público: el caso de las coronapps en América Latina (Policy Report No. 1, Serie 1: TIC en tiempos de Covid-19). Centro Latam Digital. https://centrolatam.digital/publicacion/coronapps/

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (2011). *Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar".* Naciones Unidas. https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

(2021). *Artificial intelligence risks to privacy demand urgent action –Bachelet*. https://www.ohchr.org/en/2021/09artificial-intelligence-risks-privacy-demand-urgen t-action-bachelet

Palacios, L., Forero, V., & Labarthe, S. (2024). *Fiscal Watson: estudio del uso de Inteligencia Artificial en la Fiscalía General de la Nación en Colombia.* Derechos Digitales.

Ricaurte, P., & Nájera, J. (2024). *SATPE*: *análisis del sistema predictivo para la prevención del abandono escolar del estado de Guanajuato*. Derechos Digitales

Ruiz Nicolini, J. P., Kunst, M., & Dias, J. M. (2024). *Usos inteligentes de datos en el Estado.* Fundar. https://fund.ar/wp-content/uploads/2024/09/Fundar_Usos_inteligentes_de_datos_en_el_Estado_CC-BY-NC-ND-4.0-2.pdf

Saavedra, V., & Upegui, J. C. (2021). *PretorIA y la automatización del procesamiento de causas de derechos humanos*. Derechos Digitales.

Sequera, M., & Cuevas, M. (2024). *EmpleaPY: Investigación sobre la automatización de procesos para las políticas de empleo en Paraguay*. Derechos Digitales.

Tavares, C., Fonteles, J., Simão, B., & Valente, M. (2022). *El Auxilio de Emergencia en Brasil: Desafíos en la implementación de una política de protección social datificada.* Derechos Digitales.

Tedic (2024) "Última versión del proyecto de ley de datos personales en Paraguay: Un trabajo colectivo y participativo". Tedic. Disponible en: https://www.tedic.org/ultima-version-del-proyecto-de-ley-de-datos-personales-en-paraguay/

Yael, D. (2021) *Coronavirus UY y la tecnología como solución a la pandemia*. Derechos Digitales.

Valderrama, M. (2021). *Sistema Alerta Niñez: IA e inclusión en Chile.* Derechos Digitales.

Velasco Fuentes, P. & Venturini, J. (2021) *Decisiones automatizadas en la función pública en América Latina: Una aproximación comparada a su aplicación en Brasil, Chile, Colombia y Uruguay*. Derechos Digitales.