

Inteligência Artificial no
Estado: um estudo coletivo
sobre experiências e
riscos para os direitos
humanos

INTELIGÊNCIA ARTIFICIAL NO ESTADO: ESTUDIO COLECTIVO SOBRE EXPERIENCIAS Y RIESGOS PARA LOS DERECHOS HUMANOS

Este relatório foi produzido pela Derechos Digitales, uma organização independente e sem fins lucrativos fundada em 2005. Sua missão é defender, promover e fortalecer os direitos fundamentais nos ambientes digitais na América Latina. Para mais informações sobre este projeto, visite <https://ia.derechosdigitales.org/>.



Supervisão geral: Jamila Venturini e Juan Carlos Lara

Autor: Juan Manuel García

Revisão: Paloma Lara Castro e Juan Carlos Lara

Tradução para inglês e português: Urgas Traductoras

Design: Alter Studio

Citação sugerida: García, J.M. (2024). Inteligência Artificial no Estado: Um Estudo Coletivo sobre Experiências e Riscos aos Direitos Humanos. Derechos Digitales.

Novembro de 2024



Este trabalho está disponível sob uma Licença Creative Commons Atribuição 4.0 Internacional.
<https://creativecommons.org/licenses/by/4.0/deed.en>

SUMÁRIO

Introdução	3
I. A Inteligência Artificial como artefato sociotécnico	3
II. Metodologia para análise da implementação da Inteligência Artificial	5
1. Marcos normativos aplicáveis	7
Tratados internacionais de direitos humanos	7
Proteção de Dados Pessoais e Acesso à Informação	10
2. Usos da Inteligência Artificial no Estado	12
Emprego	12
Seguridade social	15
Segurança pública	18
Justiça	19
Educação	21
Gestão de procedimentos e serviços	22
3. Análise e discussão: questões associadas ao uso e processamento automatizado de dados pelo Estado como instrumento de políticas públicas	23
O papel da pandemia: o uso da tecnologia para o gerenciamento massivo de dados	23
Considerações sobre proteção de dados pessoais	27
Problemas no uso automatizado de dados e algoritmos	28
Contrapesos democráticos: o papel dos órgãos de controle e da justiça	30
Conclusões	32
Bibliografia	35

INTELIGÊNCIA ARTIFICIAL NO ESTADO: UM ESTUDO COLETIVO SOBRE EXPERIÊNCIAS E RISCOS PARA OS DIREITOS HUMANOS

INTRODUÇÃO

I. A INTELIGÊNCIA ARTIFICIAL COMO ARTEFATO SOCIOTÉCNICO

A Inteligência Artificial já faz parte do conjunto de ferramentas à disposição do poder público para a formulação e a execução das políticas públicas. A frequente percepção dessas tecnologias, centrada principalmente na sua utilidade em dar mais eficiência aos processos, tem uma influência significativa no momento de decisão de sua aplicação no setor público. Nesse sentido, essas ferramentas são implementadas para tomar decisões relativas, por exemplo, a qual setor da população dar prioridade em uma determinada política ou quais pessoas podem potencialmente precisar de mais apoio do Estado numa determinada situação, entre outros exemplos. A este respeito, surgem preocupações quanto às implicações da utilização dessas tecnologias para o exercício dos direitos fundamentais. Essa preocupação se dá independentemente das técnicas específicas utilizadas que se enquadram no guarda-chuva conceitual de IA, como modelos de Processamento de Linguagem Natural (NLP), aprendizado de máquina (ML), sistemas preditivos de risco e processos automatizados de decisão (ADM).¹

Para se aprofundar no tema e fornecer evidências sobre esses processos, desde 2019 a Derechos Digitales analisa o problema no âmbito do programa *Inteligência Artificial e Inclusão*, no qual trabalhamos com pesquisadoras de diferentes países da América Latina para analisar as áreas em que o Estado usa essas tecnologias, as particularidades de seu uso e os riscos potenciais para os direitos humanos. Essas investigações assumiram a forma de estudos de caso, desenvolvidos conforme uma metodologia que contemplou

¹ Os acrônimos derivam dos nomes em inglês –respectivamente, *Natural Language Processing*, *Machine Learning* e *Automated Decision-Making*.

múltiplas dimensões de análise comuns a todos eles, com Os acrônimos derivam dos nomes em inglês – respectivamente, Natural Language Processing, Machine Learning e Automated Decision-Making. um interesse especial no impacto potencial sobre os direitos das pessoas. Tratam-se de estudos exploratórios que buscam fornecer evidências sobre uma atividade ainda incipiente, mas em aceleração.

O principal insumo para o desenvolvimento técnico de tecnologias baseadas em IA são os dados. No entanto, os Estados da América Latina têm dificuldades em manter práticas sólidas de uso, gerenciamento e armazenamento de dados, em parte devido a problemas como fragmentação de bancos de dados, heterogeneidade na perspectiva sobre os dados entre os órgãos estatais, diversidade de sistemas informáticos e falta de uma linguagem comum (Fundar, 2024). Isso representa um problema adicional quando se considera que, por trás dos dados usados pela IA na estrutura da gestão estatal, há pessoas que estão procurando emprego, em situação de necessidade que as permitiria receber uma pensão estatal, estudando em uma instituição pública ou usando um serviço básico, entre outras coisas.

Os direitos dessas e de todas as pessoas são garantidos por marcos internacionais de direitos humanos e pela legislação local, que estabelecem obrigações e limites para o Estado no processamento de dados – obrigações e limites que variam dependendo se os dados são enquadrados como pessoais ou públicos, variando também as condições para o uso equitativo no fornecimento de recursos e serviços. Dessa forma, este artigo pretende, com base nas evidências obtidas no decorrer do programa *Inteligência Artificial e Inclusão*, analisar efetivamente como o Estado utiliza esse tipo de tecnologia no exercício das suas funções perante a população.

Como enquadramento geral para análise, é necessário considerar que a geração dos dados processados e analisados por tecnologias baseadas em IA não é neutra. Como Buschmann (2021, p. 41) destaca em sua análise do Sistema de Previsão de Crimes Urbanos implementado no Chile, cada dado implica uma cadeia social de produção que pode incorporar vieses e perspectivas contextuais. Isso significa que os bancos de dados podem ser compostos por dados que registram situações irregulares ou imprecisas, resultando em um sistema tendencioso reprodutor de práticas discriminatórias.

Assim, para entender seu possível impacto sobre os direitos fundamentais, não basta analisar a tecnologia em si, ou seja, examinar os algoritmos e processos de automação implementados, pois isso não é feito de forma isolada. As políticas que usam a IA como instrumento estão inseridas em contextos sociais e políticos específicos, em países com composição demográfica diversa, estruturas regulatórias particulares, características

democráticas vinculadas a processos históricos e gestões governamentais que respondem à situação específica de cada território. Assim, um dos pontos centrais deste artigo é entender como uma resposta para um problema público é articulada em uma rede sociotécnica, envolvendo agentes humanos e não humanos em um determinado contexto histórico e institucional (Velasco e Venturini, 2021, p. 11).

Com essas premissas como base, o artigo está dividido em três partes. Primeiro, uma síntese das estruturas normativas aplicáveis para garantir os direitos fundamentais das pessoas no contexto do uso de tecnologias baseadas em Inteligência Artificial pelo Estado. Em seguida, há uma descrição dos dez casos de uso analisados no programa *Inteligência Artificial e Inclusão*. Por fim, uma análise das formas pelas quais os usos apresentam riscos aos direitos humanos, conforme as normas e as características específicas deles.

II. METODOLOGIA PARA ANÁLISE DA IMPLEMENTAÇÃO DA INTELIGÊNCIA ARTIFICIAL

Conforme mencionado, dada a natureza sociotécnica do desenvolvimento e da implementação dessas tecnologias, para compreender seu possível impacto sobre os direitos, é necessário entender o contexto de sua aplicação, a população sobre a qual pretende operar, o marco regulatório aplicável a essa jurisdição, as práticas de uso de dados desenvolvidas por esses governos, entre outras questões contextuais. Nesse sentido, os dez estudos de caso foram analisados a partir de uma metodologia multidimensional, que visa levar em conta a multiplicidade de fatores envolvidos no impacto potencial sobre os direitos das pessoas.

Essa metodologia, desenvolvida pela Derechos Digitales para este projeto, possui cinco dimensões:

1. Contexto nacional de implementação: busca entender as características sociodemográficas e tecnológicas do país onde os sistemas de Inteligência Artificial são implementados. São avaliados fatores como a distribuição da população, o acesso a tecnologias e as condições socioeconômicas que influenciam na eficácia do uso da IA pelo Estado;

2. Contexto regulatório e institucional: examina o marco legal e institucional que regula o uso da IA no Estado. Isso inclui a existência de leis, normativas, instituições especializadas e mecanismos de supervisão criados para garantir que o desenvolvimento e o uso da tecnologia respeitem direitos;

3. Infraestrutura de dados: analisa os recursos tecnológicos e de dados que dão suporte aos sistemas estatais de IA, como a qualidade das bases de dados, sua interoperabilidade e a presença de mecanismos para proteção da privacidade e da segurança da informação. Um dos pontos de interesse reside nas características dos dados, principalmente no que diz respeito à existência de dados pessoais nas bases que serão analisadas e processadas;

4. Processo de tomada de decisões: explora como os sistemas de IA são integrados aos processos de tomada de decisões pelo Estado, considerando a participação de agentes humanos, a transparência dos critérios usados e os mecanismos de prestação de contas;

5. Desenho tecnológico: concentra-se nas características técnicas e funcionais dos sistemas de IA implementados pelo Estado, incluindo seus objetivos, capacidades e possíveis vieses no seu desenvolvimento. Essa dimensão busca analisar se os sistemas implementados foram projetados segundo as necessidades e os objetivos da política pública.

Os estudos foram desenvolvidos por pesquisadoras dos próprios países a que os casos dizem respeito. Elas trabalharam de forma individual e em equipe, algumas em nome de uma organização e outra sem afiliação institucional. As pesquisadoras vêm da academia, da sociedade civil e também do ativismo. Essa diversidade mostra a pluralidade de pessoas interessadas e envolvidas na agenda que pretende impulsionar um uso mais democrático das tecnologias, com respeito aos direitos humanos.

Apesar de os olhares sobre os casos partirem de perspectivas diversas, as dificuldades que surgiram na implementação da metodologia foram comuns a todas as pesquisas. A primeira delas foi a falta de informações disponíveis sobre os casos. A primeira etapa para a seleção dos estudos a serem realizados foi um mapeamento feito pela Derechos Digitales a partir de pesquisa em fontes abertas de casos de uso de IA na América Latina. Foram utilizados motores de busca na web aberta. Também foram realizadas pesquisas em publicações específicas de diferentes entidades governamentais e analisados relatórios especializados de organizações internacionais e programas de financiamento para o uso da IA no Estado, entre outros métodos. As informações encontradas eram, geralmente, incompletas e fragmentadas, o que representou um desafio inicial devido à dependência de informações fornecidas por fontes oficiais de diferentes governos.

Nesse sentido, o segundo desafio decorreu das dificuldades em acessar dados de fontes oficiais. As pesquisadoras identificaram pedidos de acesso à informação

como um recurso fundamental para a análise das dimensões 3, 4 e 5. No entanto, as respostas às solicitações frequentemente chegavam incompletas e atrasadas, dificultando as pesquisas. Além disso, alguns dos representantes do governo relutaram em participar das investigações como fontes oficiais.

A última dificuldade que merece ser mencionada decorre da natureza efêmera de algumas das políticas encontradas. Durante a etapa de mapeamento, foram detectadas várias políticas que usavam ou alegavam usar a IA como instrumento central. Entretanto, ao buscar mais informações, foi observado que muitas delas foram descontinuadas ou interrompidas por dois motivos. O primeiro é a falta de financiamento após a fase piloto. O segundo é o resultado de mudanças na gestão governamental nos últimos anos, com consequentes alterações nos planos de gestão e nas prioridades de governo.

1. MARCOS NORMATIVOS APLICÁVEIS

A implementação de tecnologias baseadas em Inteligência Artificial pelo Estado apresenta desafios significativos em termos de proteção de direitos fundamentais, de modo que é essencial fazer referência aos marcos normativos aplicáveis. Esta seção aborda inicialmente as obrigações decorrentes de tratados internacionais de direitos humanos, como a Convenção Americana sobre Direitos Humanos (CADH) e o Protocolo de San Salvador (Protocolo Adicional à Convenção Americana sobre Direitos Humanos em Matéria de Direitos Econômicos, Sociais e Culturais), e sua relação com os princípios de legalidade, necessidade e proporcionalidade no uso da IA. Também examina as normas específicas sobre proteção de dados pessoais e acesso à informação em diferentes países da região, destacando os avanços, as deficiências e sua interseção com os projetos de regulação da IA. O objetivo é fornecer uma visão geral abrangente das obrigações legais e regulatórias que os Estados devem cumprir para garantir a proteção dos direitos em face do uso crescente dessas tecnologias.

Tratados internacionais de direitos humanos

Conforme mencionado anteriormente, uma das perguntas que o projeto *Inteligência Artificial e Inclusão* busca responder é até que ponto os Estados consideram os critérios de legalidade, necessidade e proporcionalidade ao implementar políticas baseadas em IA. Essa pergunta busca entender como os Estados garantem as disposições estabelecidas pelos padrões do sistema interamericano de direitos

humanos, especificamente as obrigações derivadas da CADH, do Protocolo de San Salvador e das decisões da Corte Interamericana de Direitos Humanos.

Os impactos do uso da Inteligência Artificial nos direitos humanos já foram reconhecidos em várias resoluções no âmbito internacional. A recente resolução A/HRC/RES/48/4 do Conselho de Direitos Humanos da ONU sobre o direito à privacidade na era digital delineou alguns dos riscos apresentados pela adoção da Inteligência Artificial para o exercício dos direitos humanos, que ocorrem “principalmente quando [a IA] é usada para identificação, rastreamento, criação de perfis, reconhecimento facial, previsão de comportamento e pontuação de indivíduos”. A resolução estabelece que os Estados devem respeitar os direitos humanos na implementação desses sistemas e adotar medidas preventivas e recursos eficazes em caso de violações e abusos do direito à privacidade, especialmente com mulheres, crianças e pessoas em condições de vulnerabilidade.

Nessa linha, as obrigações estabelecidas em tratados internacionais são precisas com relação aos deveres que recaem sobre os Estados ao incorporar tecnologias baseadas em IA. Para resumir essas obrigações, usaremos a análise realizada por Alimonti e de Alcântara (2024), que fornece uma perspectiva clara num relatório recente publicado pela *Electronic Frontier Foundation*, destacando os deveres dos Estados na incorporação de tecnologias baseadas em IA. Essas são algumas das implicações mencionadas pelas autoras:

- **Proteção dos direitos humanos:** os Estados devem garantir que o uso de sistemas de IA não viole os direitos humanos, conforme a CADH. Além disso, a formulação de políticas que incorporam a IA deve seguir uma abordagem de direitos humanos, orientada pelos princípios da CADH e do Protocolo de San Salvador (artigo 2);
- **Participação social e transparência:** é essencial que os processos de tomada de decisão que envolvem IA sejam transparentes e permitam a participação significativa, segundo o direito à informação e à participação consagrado na CADH;
- **Avaliação prévia do impacto sobre os direitos humanos:** antes de adotar um sistema de IA, os Estados devem realizar uma avaliação abrangente que considere sua pertinência, conforme as obrigações estabelecidas na CADH e no Protocolo de San Salvador. Além disso, o relatório do Alto Comissariado das Nações Unidas para os Direitos Humanos destaca a necessidade de garantir que essas ferramentas estejam em total acordo com o direito internacional dos direitos humanos, e recomenda a moratória, ou até mesmo a proibição, de tecnologias que não possam ser usadas

de forma compatível com esses padrões (OHCHR, 2021). Por outro lado, os Estados devem estabelecer mecanismos adequados para monitorar o uso da IA no setor público, segundo o dever de prestação de contas estabelecido na CADH;

- **Proteção de grupos em situação de vulnerabilidade:** deve ser dada atenção especial ao impacto diferenciado que o uso da IA pode ter sobre grupos historicamente discriminados, em conformidade com os princípios de igualdade e não discriminação da CADH;
- **Garantias para assegurar o princípio da não discriminação:** as políticas que usam IA devem ser formuladas para prevenir a discriminação, segundo o artigo 1.1 da CADH, que estabelece a obrigação de respeitar e garantir os direitos.

Por fim, dado o peso das iniciativas desenvolvidas pelo setor privado na agenda da IA, é importante destacar que, mesmo que as ferramentas de IA sejam desenvolvidas por entidades privadas, os Estados continuam responsáveis por garantir que seu uso respeite as obrigações mencionadas acima, conforme as obrigações derivadas da CADH e do Protocolo de San Salvador. Essa responsabilidade estatal se estende não apenas ao uso direto dessas ferramentas, mas também ao conteúdo de contratações, licenças ou qualquer outro tipo de formalização acordada com as empresas fornecedoras. Nesse sentido, os Estados devem garantir que os dados coletados, armazenados e processados nesses sistemas atendam aos padrões adequados de proteção e segurança.

Por sua vez, as empresas privadas, como agentes chave no desenvolvimento e implementação dessas tecnologias, têm responsabilidades específicas de proteção aos direitos humanos. De acordo com os Princípios Orientadores das Nações Unidas sobre Empresas e Direitos Humanos, elas devem identificar, prevenir, mitigar e, quando necessário, remediar os impactos adversos das suas operações sobre os direitos humanos, agindo de forma responsável em todos os estágios do ciclo de vida das suas ferramentas de IA (OHCHR, 2011).

Esse resumo procura destacar a existência de um marco normativo internacional que protege a população dos usos potencialmente prejudiciais da tecnologia. Os marcos internacionais, de caráter obrigatório para os Estados, são particularmente relevantes em relação a outros instrumentos internacionais que, no campo da IA, são de alta relevância. Aqui nos referimos a recomendações e princípios éticos sobre IA, os quais, embora possam fornecer uma estrutura para ação, não representam por si só fontes de obrigações vinculantes para os Estados.

Proteção de Dados Pessoais e Acesso à Informação

Segundo os marcos internacionais de direitos humanos, cada país deve desenvolver normas específicas para proteger os direitos da população, de acordo com suas obrigações internacionais. Isso inclui a incorporação na legislação nacional dos direitos e obrigações reconhecidos em tratados internacionais de forma clara e efetiva. Também é essencial que as regulações nacionais, como as leis de Proteção de Dados Pessoais (PDP) e de Acesso à Informação Pública, sejam compatíveis com as disposições internacionais, garantindo um quadro de proteção alinhado aos padrões de direitos humanos. Nesse sentido, embora a situação na região seja dispar e esteja em evolução, esses marcos representam um ponto de partida, e não um objetivo final, para assegurar a proteção de direitos fundamentais.

No Chile, até recentemente, a legislação de PDP estava enquadrada na Lei de Proteção da Vida Privada, promulgada em 1999 como Lei N° 19.628, que regulava o processamento de dados pessoais em registros ou bancos de dados. Apesar de essa ter sido uma das primeiras leis de proteção de dados na América Latina, como aponta Valderrama (2021), ela foi criticada por rapidamente ter se tornado desatualizada e por sua ineficácia em proteger adequadamente os indivíduos contra o mau uso de seus dados por terceiros. No entanto, o congresso chileno, em agosto de 2024, aprovou um novo capítulo para a Lei de Proteção de Dados Pessoais, que oferece um contexto específico para o seu tratamento e cria a Agência de Proteção de Dados Pessoais. Isso representa uma melhora da situação regulatória do país em comparação com aquela analisada nos casos, anos antes.

Em paralelo, o Brasil também conta com uma regulação recente. A Lei Geral de Proteção de Dados (LGPD), promulgada em 2018 e em vigor desde 2020, estabelece um marco legal para a proteção de dados pessoais. Possui semelhanças importantes com o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia, assim como a nova legislação chilena. Conforme analisado por Cardoso et al. (2021), ela se aplica a qualquer atividade de tratamento de dados pessoais realizada no Brasil e define dados pessoais como informações relacionadas a pessoas identificadas ou identificáveis, incluindo dados sensíveis. A lei criou a Autoridade Nacional de Proteção de Dados (ANPD), responsável por supervisionar sua aplicação e aplicar sanções em caso de descumprimento.

Assim como no Chile e no Brasil há normas recentes², na Argentina existe um projeto de lei³ criado pela Agência de Acesso a Informações Públicas com a participação de

2 No momento da finalização deste relatório, a nova lei chilena está prestes a ser promulgada e, com isso, inicia-se um período de dois anos de vacância a partir de sua publicação até que esteja totalmente em vigor.

3 Para mais informações: <https://www.argentina.gob.ar/aaip/datospersonales/proyecto-ley-datos-personales>.

empresas, instituições públicas, organizações da sociedade civil e academia. O objetivo de sua criação foi atualizar a legislação vigente, a Lei Nº 25.326, aprovada no ano 2000, quase um quarto de século atrás. O projeto de lei, porém, está parado em comissões desde agosto de 2023, sem previsão de debate em sessões plenárias.

Por outro lado, no outro extremo da escala, como afirmam Sequera e Cuevas (2024), o Paraguai não tem uma lei de proteção de dados pessoais. O principal marco aplicável é a Lei Nº 6534/2020, que se refere especificamente à proteção de dados pessoais de crédito, mas não abrange a proteção de dados em geral. Vale a pena destacar o papel da Coalizão para a Proteção de Dados Pessoais no Paraguai, um grupo que tem trabalhado ativamente desde 2016 para promover a criação de um marco legal abrangente para regular o processamento de dados pessoais no país. Em 2021, a coalizão elaborou uma proposta legislativa, que ainda não foi discutida no parlamento, embora, ao longo de 2023, a proposta tenha sido incluída na pauta da Câmara dos Deputados em quatro sessões diferentes (TEDIC, 2024).

Como podemos ver, a situação da proteção de dados pessoais na região não é homogênea. Isso é relevante quando se considera a complementaridade dessa legislação com alguns projetos de regulação específicos para IA, atualmente em discussão em diferentes países da região. Esse é o caso, por exemplo, de projetos em discussão no Chile e no Brasil, os quais incorporam uma abordagem de risco semelhante à da lei de IA aprovada pelo Parlamento Europeu. Vale mencionar, como referência, que essa normativa europeia, a qual funciona de forma complementar ao RGPD, classificaria alguns dos casos analisados como “sistemas de alto risco”, já que essa categoria inclui, por exemplo, sistemas automatizados de acesso a benefícios fornecidos pelo Estado, e sistemas utilizados para a gestão de políticas de emprego, de segurança e de administração da justiça.⁴

Por outro lado, conforme mencionado na seção metodológica, a pesquisa aponta para a necessidade de aprimorar as práticas de acesso à informação por parte dos governos da região em relação ao uso da IA e das características desse uso para o desenvolvimento de suas funções, sejam essas informações fornecidas de forma proativa ou passiva, com base em uma solicitação formalmente enviada.

As normas sobre acesso a informações públicas em países como Chile, Argentina, Uruguai e México fornecem um marco para ambos os casos de acesso a elas. Ainda que não existam marcos específicos para regular o fornecimento de informações que se refiram

especificamente à Inteligência Artificial, isso não deveria ser um problema, pois os Estados são obrigados a garantir a divulgação dessas informações com base nas normas gerais sobre transparência e acesso a informações públicas. Pelo contrário, a devida aplicação desses marcos facilitaria a transparência pública na implementação de IA.

2. USOS DA INTELIGÊNCIA ARTIFICIAL NO ESTADO

Nesta seção, analisaremos como os diferentes Estados da região usam as tecnologias baseadas em IA como um instrumento para a implementação de políticas públicas, com base nas evidências geradas pelo projeto *Inteligência Artificial e Inclusão*, conforme mencionado acima. No centro dessa linha programática está o interesse no possível impacto sobre os direitos humanos decorrente do uso da IA pelo Estado. Especificamente, procura-se responder à pergunta: como os governos da América Latina estão implementando a Inteligência Artificial e quais são seus impactos no desenvolvimento, na inclusão e nos direitos humanos? E, além disso, como eles consideram os critérios de legalidade, necessidade e proporcionalidade?

Os casos analisados mostram exemplos de uso em áreas sensíveis da administração pública, como emprego, seguridade social, segurança pública, educação e gerenciamento de processos, bem como usos na administração da justiça. Forneceremos detalhes sobre cada um deles. Cada caso e sua descrição incluirá caixas explicativas sobre as características técnicas das tecnologias utilizadas, dos bancos de dados ou empresas de tecnologia envolvidas, quando for relevante para a compreensão.

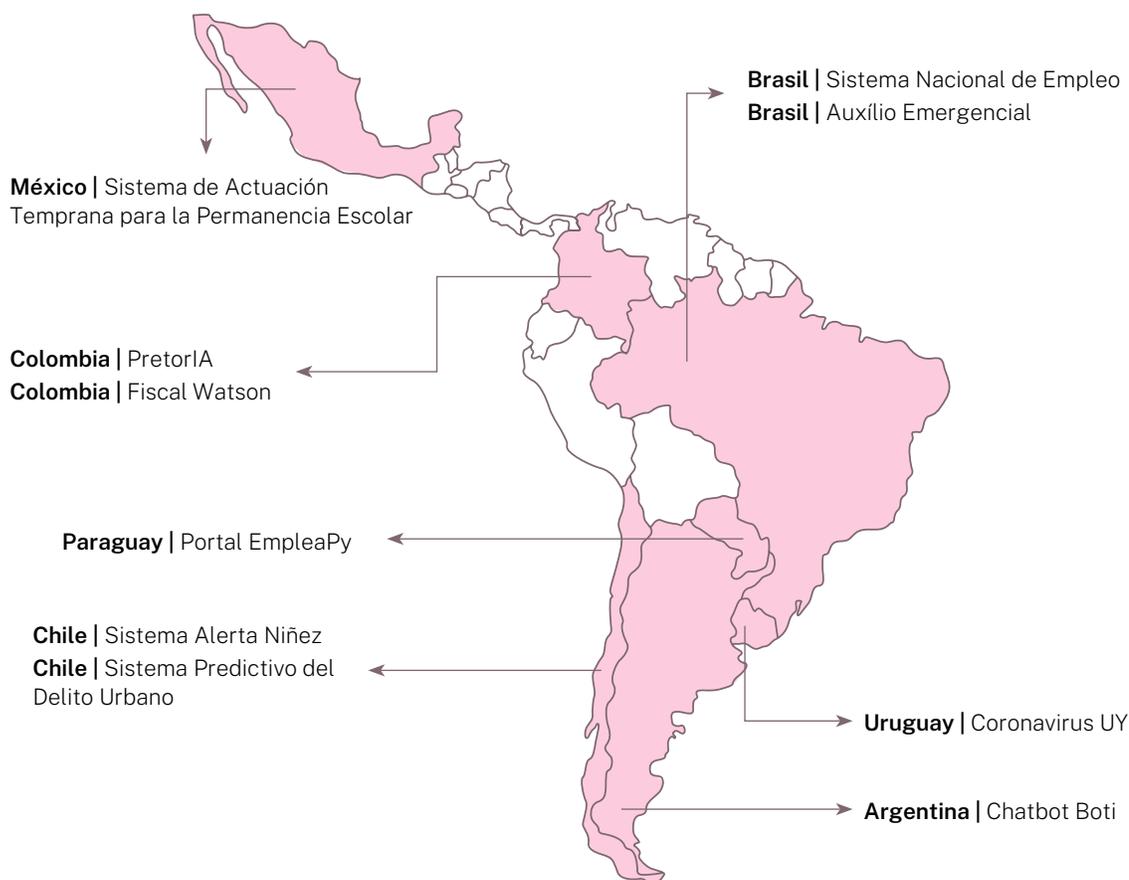
EMPREGO

A Dataprev, Empresa Brasileira de Tecnologia e Informações da Previdência Social, foi criada pela Lei Nº 6.125 em 1974. É uma empresa pública vinculada ao Ministério da Economia, responsável pela gestão do Banco de Dados Sociais Brasileiro. Fornece ferramentas tecnológicas para a implementação de políticas sociais do Estado brasileiro.

Em matéria de emprego, foram analisados dois casos: a incorporação da IA na estrutura do **Sistema Nacional de Emprego (SINE)** no Brasil, uma política de trabalho ativa desde 1975; e a automação de processos dentro do programa EmpleaPy, gerenciado pelo Ministério do Trabalho, Emprego e Seguridade Social (MTESS) do Paraguai. Ambos os casos se tratam de políticas de intermediação trabalhista, cujo objetivo

é facilitar a conexão entre as pessoas que procuram emprego e as empresas e organizações que precisam contratar trabalhadoras/es.

Em 2019, o Sistema Nacional de Emprego passou por uma transformação significativa com a introdução do “Novo SINE”. Esse processo de reestruturação buscou modernizar o sistema por meio da implementação de ferramentas tecnológicas como a IA para a análise de correspondências entre quem procura emprego e as vagas ofertadas, o uso e a importância de dados digitais com informações do mercado de trabalho e parcerias com o setor privado (Bruno et al. 2021, p. 10).



Especificamente, a implementação de ferramentas de IA está enquadrada no Plano de Transformação Digital do SINE, iniciado em 2019 pela Secretaria de Políticas Públicas de Emprego (SPPE), como resultado do Novo SINE e, sobretudo, do relacionamento mais amplo entre o governo federal brasileiro e a Microsoft (Bruno et al. 2021, p. 14). O projeto envolve o uso de ferramentas de Inteligência Artificial fornecidas pela Microsoft ao governo brasileiro para os setores de emprego e sustentabilidade. A oferta da Microsoft para o setor de emprego envolve a implementação de IA para intermediação de mão de obra no Portal de Vagas do SINE, o Portal Emprega Brasil, e a qualificação de trabalhadoras/es por meio da Escola do Trabalhador 4.0. A Escola é uma plataforma de ensino à distância desenvolvida pela Secretaria Especial de Produtividade, Emprego e Competitividade do Ministério da Economia (SEPEC/ME) em parceria com a Agência Brasileira de Desenvolvimento Industrial (ABDI), que inclui cursos da Microsoft através da ferramenta de formação da Microsoft Community Training (Bruno et al. 2021, p. 14).

Além disso, a empresa estatal Dataprev, por meio de sua infraestrutura tecnológica, permite que empresas privadas acessem dados anonimizados de trabalhadores/as com registro no SINE. Isso ocorre no âmbito do projeto SINE Aberto, parte do processo de modernização mencionado anteriormente, que visa fornecer acesso ao banco de dados de trabalhadores/as com registro no SINE para empresas privadas e outras instituições do segmento de intermediação do trabalho (Bruno et al., 2021,12).

Tanto o SINE quanto o EmpleaPy usam técnicas de Matching Semântico (correlação semântica) para encontrar correspondências entre quem oferece e quem procura emprego. Essa é uma técnica informática para identificar informações semanticamente relacionadas. Dadas duas estruturas gráficas, por exemplo, classificações, bancos de dados de taxonomia e XML Schemas e ontologias, a correspondência é um operador que identifica quais nós das duas estruturas correspondem de forma semântica um ao outro.

O vínculo entre a Microsoft e o governo do Brasil é baseado em um Acordo de Cooperação Técnica. De acordo com as pesquisadoras, o instrumento envolve o uso de dados, tecnologia digital e Inteligência Artificial, com o apoio de ferramentas e licenças do Microsoft Dynamics, PowerBI Premium e recursos de Inteligência Artificial da nuvem Azure. O plano de trabalho estabelece que a ferramenta tecnológica usará o módulo Customer Insights do Microsoft Dynamics 365 para a unificação e o processamento de dados, tendo como resultado esperado um melhor entendimento sobre as pessoas trabalhadoras e as vagas. (Bruno et. al. 2021, p. 49).

Da mesma forma, o caso da **EmpleaPy** no Paraguai busca automatizar os processos para

conectar empregadores e candidatos. Sua versão inicial, conhecida como ParaEmpleo, foi criada pela empresa suíça Janzz Technology. Posteriormente, o MTESS gerou uma nova versão, o EmpleaPy, que incorpora a tomada de decisões automatizada. Essa é a versão que estava vigente na época do estudo (Sequera e Cuevas, 2024).

Em relação à atualização e melhoria do software da Janzz Technology pelo MTESS, as autoras da pesquisa constataram, em entrevista com a área técnica do Ministério, que a nova versão foi desenvolvida internamente, do zero, com financiamento estatal (Sequera e Cuevas, 2024, p. 16). Essa versão reaproveitou a maneira como a Janzz Technology processava dados de forma genérica e a ajustou às suas necessidades específicas e às novas funcionalidades.

Ao mesmo tempo, fontes da área técnica consultadas pelas pesquisadoras afirmaram que a plataforma EmpleaPy ainda não usa Inteligência Artificial. Ao invés disso, tem um processamento complexo e automatizado de determinados processos algorítmicos, facilitando o gerenciamento da identificação da pessoa, o arquivo de perfil tanto de pessoas quanto de empresas e, em seguida, o agrupamento e a sugestão de palavras-chave e palavras comuns usadas por ambos. Inclusive, afirmam que realizam o processo de agrupamento manualmente e que o único processo automatizado é a consulta e a validação do perfil da pessoa usuária (Sequera e Cuevas, 2024, p. 16).

SEGURIDADE SOCIAL

O CadÚnico, criado em 2001, é um banco de dados para a identificação e caracterização socioeconômica das famílias brasileiras de baixa renda. É utilizado em mais de trinta políticas públicas no Brasil, sendo seu principal instrumento a seleção de famílias de baixa renda para os programas que compõem a Assistência Social Federal.

Três casos foram analisados nessa área de competência do serviço público: o programa Auxílio Emergencial no Brasil, o aplicativo Coronavirus UY no Uruguai e, por fim, o Sistema Alerta Niñez (SAN) no Chile.

O **Auxílio Emergencial (AE)** é uma política de transferência de renda cujo objetivo é mitigar os efeitos econômicos e sociais da pandemia de COVID-19 e permitir que a população em situação de vulnerabilidade mantenha o acesso a bens de consumo, especialmente alimentos (Tavares et al., 2022).

O AE foi concedido automaticamente tanto às pessoas beneficiárias do Programa Bolsa Família⁵ quanto às pessoas registradas no banco de dados do CadÚnico, caso atendessem aos critérios de elegibilidade do programa. Em relação às políticas públicas já existentes no país, o AE aproveitou a estrutura preexistente de programas de transferência de renda, como o Programa Bolsa Família, para atingir um novo público, que não era beneficiário de nenhuma política social (o chamado público ExtraCad); além disso, foram implementadas novas medidas e tecnologias (Tavares et al., 2022, p. 14).

O Auxílio Emergencial é composto por um fluxo intenso de dados, que percorre todos os estágios do programa. A seleção das pessoas beneficiárias é automatizada, realizada pela já mencionada empresa Dataprev, que cruza múltiplas bases de dados de diferentes órgãos governamentais com os dados do CadÚnico e com os requerimentos para concessão do benefício do público do ExtraCad, realizados por meio do aplicativo Auxílio Emergencial (Tavares et al., 2022, p. 19).

Um modelo preditivo de risco (Predictive Risk Model, PRM) é uma ferramenta que usa padrões estabelecidos em bancos de dados para gerar automaticamente uma probabilidade (ou pontuação de risco) de que um evento específico aconteça com um indivíduo no futuro. Como os PRM costumam usar dados coletados para outras finalidades (por exemplo, bancos de dados administrativos do governo) e podem ser automatizados, eles podem examinar de maneira eficiente grandes populações para identificar um pequeno número de indivíduos com alto risco. (AUT & UAI, 2019, p. 107; citado em Valderrama, 2021).

O **Coronavirus UY**, administrado pelo Ministério da Saúde Pública do Uruguai (MSP), funcionou como um mecanismo de gerenciamento de informações para lidar com a pandemia de COVID-19. É um sistema informático desenvolvido a pedido de agentes públicos e privados, principalmente pela Agência de Governo Eletrônico e Sociedade da Informação e do Conhecimento (Agesic), que tem um aplicativo de celular como um de seus componentes mais importantes (Yael, 2021, p. 5).

O aplicativo Coronavirus UY foi projetado para fornecer informações públicas sobre as estatísticas de infecção do então novo coronavírus e as medidas de saúde vigentes na época. Também pretendia monitorar possíveis casos de infecção por meio da coleta de dados de autodiagnóstico, fornecer assistência médica

5 O Programa Bolsa Família, implementado pelo governo federal e ativo desde 2003, é o maior programa de transferência de renda do Brasil. Além de proporcionar renda às famílias em situação de pobreza, integra políticas públicas para ampliar o acesso a direitos básicos como saúde, educação e assistência social, articulando ações complementares em áreas como esporte, ciência e trabalho para a superação da pobreza. Para mais informações: <https://www.gov.br/mds/pt-br/acoes-e-programas/bolsa-familia>.

remota durante períodos de confinamento e, a partir de meados de 2020, alertar as pessoas usuárias sobre possíveis contatos com pessoas infectadas. O sistema centralizou essas informações para facilitar o planejamento de ações do Estado, tanto para a população em geral quanto para casos individuais, fornecendo desde recomendações de cuidados até atendimento médico por meio de telemedicina (Yael, 2021, p. 5).

O banco de dados utilizado pelo aplicativo Coronavirus UY, que centralizava os formulários epidemiológicos, estava sob a administração MSP. Cada provedor de saúde gerenciava seu próprio banco de dados de forma independente. Os registros clínicos eletrônicos de pacientes, atualizados pelas equipes médicas responsáveis, eram armazenados na instituição médica onde cada paciente recebeu tratamento. Todas as informações geradas pela equipe de saúde sobre um/a paciente deveriam ser mantidas sob a custódia da instituição em questão. Além disso, as pessoas usuárias podiam acessar seu histórico médico por meio dos portais da web dos provedores que ofereciam essa opção ou solicitá-lo diretamente com sua carteira de identidade (Yael, 2021, p. 23). Por fim, o **Sistema Alerta Niñez** pretende estimar e prever o nível de risco que crianças e adolescentes correm de sofrer qualquer violação de seus direitos, por meio da análise de dados a partir de diferentes modelos algorítmicos, a fim de antecipar e intervir precoce e preventivamente em cada caso. Na prática, o sistema gera uma **pontuação** ou “índice de risco” para cada criança e adolescente que permite que os casos sejam classificados em ordem de prioridade para as Oficinas Locais da Infância (**Oficinas Locales de Niñez - OLN**). Além disso, o sistema se tornou uma plataforma para o registro, o gerenciamento e o monitoramento dos casos de crianças e adolescentes identificados como de maior risco (Valderrama, 2021, p. 23). Os modelos preditivos foram treinados com dados de várias fontes, incluindo o SENAME, Chile Crece Contigo, o Ministério da Educação (informação de matrícula e rendimento de colégios públicos e privados no Chile), o Registro Social de Domicílios, dados censitários sobre vulnerabilidade de bairros e informações de delitos por bairro da Subsecretaria de Prevenção do Delito, calculados em raios de 300 a 1.000 metros ao redor do lar de cada criança ou adolescente (Valderrama, 2021, p. 31).

Trata-se de sistema informático desenvolvido e mantido pela Subsecretaria de Avaliação Social e implementado nas OLN da Subsecretaria da Infância, ambas subsecretarias dependentes do Ministério de Desenvolvimento Social e da Família do Chile. O papel dos modelos preditivos se reduz à realização de uma classificação inicial, segundo critérios de priorização, para estabelecer uma ordem na qual serão atendidos os casos. Essa pontuação de risco é exibida em uma coluna ao lado de outras colunas, como as de alertas territoriais e do **Chile Crece Contigo**. Embora já no cálculo das listas

se restrinja o universo de possíveis crianças e adolescentes a atender, dependerá da/o coordenador/a e das/os gestoras/es de casos de cada OLN decidir se seguirá ou não a ordem de prioridade estimada pelo instrumento preditivo (Valderrama, 2021, p. 23).

SEGURANÇA PÚBLICA

Foi analisado o **Sistema Preditivo do Crime Urbano**, desenvolvido pelo Centro de Análise e Modelagem em Segurança (CEAMOS) da Universidade do Chile junto ao Departamento de Análise Criminal (DAC) da *Carabineros de Chile*. O desenvolvimento do sistema, o qual foi implementado em 58 delegacias em todo o país, teve como objetivo prever zonas de maior risco de ocorrência de crimes para direcionar o patrulhamento policial preventivo nas cidades, definindo áreas para maior vigilância e controle. Conforme o relatório, o governo define como vigilância policial as ações “para evitar situações indesejadas ou detectá-las para neutralização”, o que se traduz nas seguintes funções operacionais: “vigilância preventiva, procedimentos policiais, fiscalização seletiva, serviços extraordinários e cumprimento de ordens judiciais” (MDS, 2013, p. 10; citado em Buschmann, 2021, p. 22).

AUPOL (Automação de Unidades Policiais) é a principal plataforma da Carabineros para registrar e armazenar dados referentes a denúncias, detenções, constâncias e infrações. Este sistema permite gerar os relatórios policiais que são entregues a juizados e promotorias.

A tecnologia usada no contexto do Sistema Preditivo do Crime Urbano se baseia na previsão de crimes, e é definida como qualquer sistema que analisa dados existentes para prever eventos criminais (Buschmann, 2021, p. 9). De acordo com a autora, os sistemas de IA, nesse contexto, usam técnicas de aprendizado de máquina e análise de dados para identificar padrões na ocorrência de crimes. Os padrões são baseados em teorias criminológicas que afirmam que o crime não é distribuído aleatoriamente, mas segue padrões ambientais, situacionais e sociais que podem ser analisados e conhecidos (Buschmann, 2021, p. 10).

O sistema de predição de crimes usa dois tipos de dados. O primeiro tipo são os casos policiais, que incluem detenções e denúncias relacionadas a delitos de maior conotação social (DMCS) agrupados na hipótese de roubo com emprego de força e violência. Os casos são registrados pela Carabineros na plataforma AUPOL, incluindo dados da/o funcionária/o que insere as denúncias e as detenções no sistema e dados de identificação pessoal das/os afetadas/os, testemunhas, denunciantes

e/ou pessoas detidas, como nome completo, número de identificação nacional, profissão, escolaridade, gênero, idade, características físicas, estatura e domicílio. O segundo tipo de dados considerados é a localização de serviços e atrações urbanas identificadas como fatores contextuais relevantes, que podem motivar e facilitar a ocorrência de um crime. Nesse último ponto, de acordo com as/os desenvolvedoras/es do sistema, é considerada a localização de bancos, pontos de ônibus, restaurantes e caixas eletrônicos (Buschmann, 2021, p. 28). Estes dados são obtidos por meio de informações registradas pela Carabineros em seu sistema de informações geográficas e de plataformas abertas colaborativas como Open Street Maps (Baloian et al., 2017; Carabineros de Chile, 2018; citado em Buschmann, 2021).

JUSTIÇA

Com relação ao setor de administração da justiça, foram analisados dois casos, ambos na Colômbia. O primeiro é o sistema PretorIA, implementado no Tribunal Constitucional, e o segundo é o **Fiscal Watson**, usado na Procuradoria Geral da Nação.

O PretorIA usa técnicas de Processamento de Linguagem Natural (NLP), que é um campo da inteligência artificial que se concentra na interação entre computadores e linguagem humana. Por meio do PLN, o sistema pode analisar, categorizar e extrair informações relevantes dos textos das sentenças de tutela. Isso inclui a marcação automática de documentos e a geração de estatísticas de casos.

O sistema **PretorIA** usa o Processamento de Linguagem Natural para apoiar o processo de seleção de tutela no Tribunal Constitucional da Colômbia. Sua principal função é classificar e rotular as sentenças de tutela de acordo com categorias previamente estabelecidas por especialistas. O sistema trabalha com textos jurídicos em espanhol e fornece informações sobre o conteúdo das sentenças, bem como dados estatísticos gerais. Quanto à sua autonomia, o PretorIA não tem a capacidade de tomar decisões judiciais. Funciona como uma ferramenta de apoio no processo de seleção de tutela, mas as decisões finais são tomadas pelas autoridades do Tribunal Constitucional. O sistema

não atua de forma independente e sua função esperada é simplificar o trabalho de análise de casos (Saavedra e Upegui, 2021, p. 5). As tutelas são ações constitucionais estabelecidas no artigo 86 da Constituição Política da Colômbia. Sua finalidade é a proteção imediata dos direitos fundamentais das pessoas ante sua violação ou ameaça de violação. Esse mecanismo permite à população solicitar a intervenção do Tribunal Constitucional ou das magistraturas para salvaguardar seus direitos fundamentais

de forma rápida e eficaz (Saavedra e Upegui, 2021, p. 18). O PretorIa obtém os dados dos arquivos de tutela enviados pelas/os juízas/es e tribunais de primeira e segunda instância ao Tribunal Constitucional. O sistema processa textos de sentenças e usa categorias definidas pela equipe do Tribunal para classificar e rotular as informações (Saavedra e Upegui, 2021, p. 46).

Na Colômbia, a Procuradoria Geral da Nação implementou o **Fiscal Watson**, uma ferramenta baseada em Inteligência Artificial desenvolvida pela IBM, para apoiar o gerenciamento de informações do Sistema Penal de Acusação Oral (SPOA). Tal sistema centraliza as informações relacionadas a investigações criminais, processos judiciais e gerenciamento de provas, entre outras. O Fiscal Watson usa algoritmos avançados para analisar dados estruturados e não estruturados, identificando padrões, tendências e possíveis conexões entre processos judiciais, visando facilitar a tomada de decisões por parte de servidoras/es judiciais (Palacios et al., 2024, p. 11).

O Fiscal Watson atua na fase inicial de investigação dos processos judiciais criminais, pesquisando e correlacionando informações de pesquisas com base em critérios predefinidos pelas pessoas usuárias. Esses critérios podem ser geográficos (local do evento) ou qualitativos (detalhes específicos do relato factual). Por exemplo, o Watson pode detectar conexões entre casos de homicídio envolvendo o mesmo perpetrador, padrões criminais semelhantes em uma região e pontos em comum no *modus operandi* de diferentes processos judiciais. Essa análise ajuda pesquisadores e pesquisadoras a obter uma visão mais ampla e a identificar possíveis vínculos que podem não ser visíveis na análise manual de grandes volumes de dados (Palacios et al., 2024, p. 13).

O SPOA, a principal fonte de informações do Fiscal Watson, é um vasto sistema de informações criminais que consolida dados de diversos bancos de dados judiciais, policiais, administrativos e outros. Esse sistema inclui módulos para registro de relatos factuais, gerenciamento de processos judiciais, distribuição de casos entre servidoras/es e consulta de casos arquivados. Um dos módulos mais relevantes para o funcionamento do Watson é o que contém os **relatos dos fatos**, ou seja, as descrições iniciais dos eventos registrados nos processos judiciais.

A tarefa de quem transcreve esses relatos é fundamental, pois qualquer omissão ou erro pode levar a resultados imprecisos, discriminatórios e incorretos na análise realizada pelo Watson (Palacios et al., 2024, p. 14).

Para garantir a segurança e a integridade dos dados, o Fiscal Watson não acessa diretamente o banco original de dados do SPOA. Em vez disso, usa uma cópia do

sistema, o que garante que as informações originais permaneçam protegidas enquanto o Watson realiza suas análises e consultas (Palacios et al., 2024, p. 16).

EDUCAÇÃO

A Secretaria de Educação de Guanajuato, no México, desenvolveu o **Sistema de Alerta Precoce para Prevenção ao Abandono Escolar (SATPE)** para reduzir a taxa de evasão nas escolas secundárias. O sistema faz parte do Pacto Social pela Educação, uma estratégia abrangente do governo de Guanajuato que busca melhorar a qualidade da educação e garantir a permanência de estudantes no sistema escolar (Ricaurte e Nájera, 2024, p. 10). O Pacto está estruturado em quatro componentes principais: garantir a frequência escolar, assegurar que ninguém se atrase em sua aprendizagem, reconhecer a figura docente e incentivar a participação das famílias no processo educacional (Ricaurte e Nájera, 2024, p. 13).

As ferramentas de inteligência empresarial (BI, business intelligence) permitem a geração de painéis de análise e visualização de dados a partir de interfaces de usuário intuitivas, o que as torna fáceis de usar por pessoas sem conhecimento técnico avançado de processamento de dados.

Os dados usados pelo SATPE vêm de várias fontes, incluindo o Sistema de Controle Escolar, que coleta informações sobre matrícula, frequência e desempenho de estudantes de escolas públicas. Também são usados dados do Catálogo Oficial de Escolas do Estado de Guanajuato (CEO), o qual fornece informações sobre as escolas do estado, e da pesquisa Coleta de Informações para Melhoria da Aprendizagem (RIMA), a qual se baseia em indicadores de aprendizagem. Além disso, são consideradas as informações a respeito do corpo docente

(Ricaurte e Nájera, 2024, p. 18). A gestão dos dados relacionados aos indicadores educacionais e ao controle escolar utilizados no SATPE é realizada por meio do software Power BI, um sistema de inteligência empresarial desenvolvido pela Microsoft (Ricaurte e Nájera, 2024, p. 21).

Os dados foram coletados por meio do Aviso de Privacidade Simplificado da Diretoria de Serviços Escolares, por meio do qual “os usuários (pais e mães, tutores e tutoras) são informados sobre as finalidades para as quais os dados das crianças e adolescentes são coletados, obtendo seu consentimento tácito e, em alguns casos, expresso”, conforme indicado pela Unidade de Transparência do Poder Executivo do Estado de Guanajuato (Ricaurte e Nájera, 2024, p. 18).

GESTÃO DE PROCEDIMENTOS E SERVIÇOS

Um chatbot é um software projetado para interagir com as pessoas simulando uma conversa humana via comandos de voz e texto, geralmente por meio da internet. Desde os primeiros programas desenvolvidos nos anos 60 até hoje, os chatbots evoluíram para serem impulsionados por algoritmos que lhes permitem aprender a partir das interações com usuárias e usuários, de modo a otimizar suas respostas futuras. (Adamopoulou et al., 2020; citado em Ferreyra, 2024).

O último estudo de caso é o **chatbot Boti**, implementado pelo Governo da Cidade de Buenos Aires (GCBA). É um assistente virtual que permite que a população interaja e obtenha informações via WhatsApp. Esse chatbot usa o Processamento de Linguagem Natural (PLN) e por ser de domínio aberto, oferece respostas sobre uma ampla variedade de tópicos, incluindo serviços governamentais, saúde e mobilidade urbana. Desde seu lançamento, o Boti evoluiu para incluir funções como assistência durante a pandemia de COVID-19, fornecendo informações sobre saúde e permitindo o acesso a serviços públicos, tornando-se um canal de centralização da comunicação entre a administração e a população (Ferreyra, 2024, p. 10-12).

Segundo o GCBA, o Boti teve um crescimento significativo desde sua implementação. Durante a pandemia de COVID-19, o Boti se tornou a principal fonte de informações oficiais sobre sintomas, prevenção e gerenciamento de horários e certificados de vacinação. Durante o primeiro trimestre de 2022, o Boti atingiu seu recorde de 26 milhões de interações mensais, tornando-se o principal canal de comunicação do GCBA com a população. No entanto, posteriormente, os números caíram para um patamar entre 2 e 5 milhões de conversas por mês, conforme declarado pelo autor com base em informações oficiais (Ferreyra, 2024, p. 6).

Esse chatbot obtém dados de várias fontes e sistemas de gerenciamento do governo da cidade. As informações para solicitações e trâmites particulares são vinculadas a outros sistemas do governo, como o Sistema de Trâmites Digitais (STD) e a plataforma de Trâmites à Distância (TAD). Esses sistemas permitem que a área competente do governo atenda às solicitações das/os usuárias/os. Além disso, o GCBA afirma que todos os dados fornecidos pelas pessoas se encontram protegidos por acordos de confidencialidade e são usados somente para executar as funcionalidades oferecidas pelo chatbot. Em situações excepcionais, as informações obtidas podem ser mantidas durante um período prolongado, conforme considerado apropriado pela administração, sempre conforme a legislação de proteção de dados (Ferreyra, 2024, p. 16).

3. ANÁLISE E DISCUSSÃO: QUESTÕES ASSOCIADAS AO USO E PROCESSAMENTO AUTOMATIZADO DE DADOS PELO ESTADO COMO INSTRUMENTO DE POLÍTICAS PÚBLICAS

Nesta seção, analisaremos algumas das implicações desses casos de uso de IA em relação a riscos para o exercício de direitos. Fatores de influência são os dados com os quais os sistemas são treinados, os dados que os sistemas utilizam e os algoritmos a partir dos quais são processados. Da mesma forma, as implicações para a proteção de dados pessoais e o acesso à informação pública serão analisadas à luz das normativas de cada país envolvido. Para tanto, primeiro é necessário abordar as implicações de um dos eventos de maior influência que ocorreu durante o desenvolvimento desta pesquisa: a pandemia de COVID-19.

O papel da pandemia: o uso da tecnologia para o gerenciamento massivo de dados

Numa pesquisa coletiva realizada pela Derechos Digitales em conjunto com o *Consortio AlSur*, foi feito um estudo sobre as implicações do uso de tecnologia durante a pandemia (Consortio AlSur, 2021). O estudo analisou as principais características dos aplicativos móveis implementados por governos em 14 países da região e expressou profunda preocupação com a falta de uma abordagem abrangente por parte dos Estados para garantir o respeito aos direitos humanos, em consonância com os padrões estabelecidos internacionalmente. Essa falha no cumprimento de suas obrigações de proteção levou, em muitos casos, à violação de direitos (Consortio AlSur, 2021, p. 65).

A falta de ações abrangentes por parte dos governos para proteger direitos levanta preocupações não apenas no uso de aplicativos móveis, mas também em relação às tecnologias analisadas neste estudo. Como o programa *Inteligência Artificial e Inclusão* começou em 2019, foi possível examinar o surgimento de novos aplicativos destinados a gerenciar aspectos relacionados à pandemia na região, bem como a expansão da área de influência de tecnologias e aplicativos já existentes. Em quatro dos dez casos analisados, a pandemia desempenhou um papel central na implementação e no crescimento das tecnologias em questão.

O aplicativo Coronavirus UY analisado por Yael (2021) é o exemplo mais claro e representativo do acima exposto. Conforme mencionado, trata-se de um aplicativo cuja função é coletar informações de forma centralizada para direcionar as ações do Estado tanto no nível geral quanto em relação a casos individuais. Ele forneceu desde recomendações de cuidados até atendimentos de telemedicina (Yael, 2021, p. 5). Essa

foi uma das iniciativas de mais destaque dentro de uma estratégia de implementação tecnológica que, além do aplicativo, incorporou vários serviços de atendimento à população por meio de sites estatais e plataformas populares como o Facebook e WhatsApp, apresentados na forma de um assistente virtual (Yael, 2021, p. 7).

O segundo exemplo é o uso de Inteligência Artificial no programa Auxílio Emergencial no Brasil. Nesse caso, a tecnologia foi usada como uma ferramenta de gestão administrativa para implementar uma política destinada a mitigar os danos econômicos e sociais causados pela pandemia. Ao contrário do Coronavírus UY, o uso da IA foi interno e limitado ao gerenciamento administrativo. Embora não tenham participado grandes empresas de tecnologia, a empresa estatal Dataprev desempenhou um papel central.

Por outro lado, a pandemia impulsionou o desenvolvimento de algumas implementações de IA já existentes. O primeiro caso a ser mencionado, também no Brasil, é o do Sistema Nacional de Emprego. O acordo de cooperação técnica que possibilitou a implementação de ferramentas de IA foi firmado em novembro de 2020 entre o governo brasileiro e a Microsoft. Ele surge como uma resposta da empresa a uma chamada pública de propostas destinada a mitigar os impactos negativos da pandemia de COVID-19 no setor produtivo do Brasil (Bruno et al., 2022, p. 6).

O último exemplo de sistema bastante impulsionado pela pandemia é o chatbot Boti, implementado pelo Governo da Cidade de Buenos Aires. O chatbot assumiu um papel preponderante com suas funções que iam desde o gerenciamento administrativo e apontamento de datas de vacinação até a criação de uma ferramenta de autodiagnóstico que funcionava por meio de uma rede neuronal capaz de classificar sons de voz, respiração e tosse analisando áudios enviados pelo WhatsApp para detectar possíveis casos suspeitos de COVID-19 (Ferreyra, 2024, p. 12). Durante o seu funcionamento no período da pandemia, as interações mensais das pessoas com o chatbot aumentaram exponencialmente, de algumas centenas de milhares para milhões, com um pico de 26 milhões no início de 2022 (Ferreyra, 2024, p. 6).

Esse cenário destaca dois pontos chave que merecem atenção. Primeiro, o papel central da Inteligência Artificial na implementação de políticas voltadas para inúmeras pessoas usuárias, como nos quatro casos mencionados acima. Segundo, a relevância dos contratos estabelecidos com grandes empresas de tecnologia para a prestação desses serviços em três dos casos, principalmente com a Meta (antigo Facebook) e a Microsoft. Dentre os dez casos analisados, as tecnologias implementadas durante a pandemia são as mais dependentes dessas grandes empresas, incluindo o Fiscal Watson, que é totalmente dependente dos serviços da IBM.

Acesso à informação pública: desafios entre a opacidade e a divulgação inadequada de dados

Conforme mencionado na introdução, uma das maiores dificuldades para a condução dos estudos de caso foi o acesso a informações e fontes que permitissem compreender como o Estado usa as tecnologias de IA.

No relatório sobre o Sistema Preditivo do Crime Urbano, Buschmann (2021, p. 9) afirma que, embora a Carabineros tenha incorporado espaços para fortalecer a transparência e a probidade administrativa—como o Departamento de Informação Pública e Lobby, o Departamento de Reclamações e Sugestões e a plataforma de estatísticas criminais STOP—, grande parte dos dados publicados não se encontram desagregados. Além disso, as informações sobre a distribuição da equipe policial no território são secretas e há pouca informação sobre os delitos cometidos por funcionários da Carabineros. Buschmann ainda afirma que as investigações sumárias dentro da Carabineros têm caráter secreto, o que foi questionado pela Convenção Interamericana de Direitos Humanos e se contrapõe ao princípio de probidade estabelecido na Constituição chilena. Por outro lado, a autora destaca um problema relacionado ao Conselho de Transparência. Afirma que seu papel fiscalizador, como o de todo órgão público, se limita a cumprir normas e não se estende à resolução de problemas sobre pedidos de acesso à informação. Isso, por sua vez, se relaciona com a necessidade de reconhecer o acesso à informação pública como um direito fundamental consagrado na Constituição (Castillo, 2009; CIDH, 2016; citados em Buschmann, 2021, p.9).

No seu estudo sobre o chatbot Boti, Ferreyra (2024, p. 4) afirma que a coleta de informações sobre o funcionamento da ferramenta, bem como os seus mecanismos de gestão interna, foi baseada em fontes abertas e em um pedido de acesso à informação apresentado perante o GCBA, “cuja imprecisão em boa parte das respostas motivou uma segunda solicitação que, no momento de finalização da pesquisa, ainda não tinha sido respondida” (Ferreyra, 2024, p. 4). Cabe ressaltar que a cidade de Buenos Aires tem uma lei de acesso à informação recentemente reformada (Lei N° 104, 2017), resultado de um processo aberto de consultas públicas. No entanto, a existência dessa lei não tem sido uma garantia de acesso efetivo às informações sobre o uso de tecnologia pelo GCBA. Outro exemplo é o do *Observatorio de Derecho Informático Argentino (O.D.I.A.)*, que fez dois pedidos de acesso à informação sobre o uso de IA em câmeras de reconhecimento facial na cidade de Buenos Aires. De acordo com fontes do Observatorio, essas duas solicitações não foram respondidas de forma satisfatória, por isso foi apresentada uma ação judicial para suspender o uso do Sistema de Reconhecimento Facial de Fugitivos da cidade de Buenos Aires. Em primeira instância,

a ação foi rejeitada, mas posteriormente o Observatorio recorreu e ampliou o processo para pedir a inconstitucionalidade do uso dessa tecnologia.⁶

Por outro lado, no caso do Auxílio Emergencial, as pesquisadoras não analisam um problema de falta de informações, mas sim de divulgação de dados pessoais, incluindo dados sensíveis, de forma contrária aos princípios de proteção de dados e aos direitos individuais. As autoras (Tavares et al., 2022, p. 33) argumentam que quaisquer atos da administração pública no Brasil estão submetidos ao princípio da transparência, por obrigação instituída originalmente no mandamento constitucional de observância ao princípio da publicidade, positivado no art. 37. Os efeitos de tal princípio na gestão pública foram consolidados em 2011 pela Lei de Acesso à Informação (Lei nº 12.527/11), na qual se estabeleceu a diretriz de que a observância da publicidade é regra geral e o sigilo a exceção. Nesse quadro, os atos e procedimentos relativos ao Auxílio se subordinam a tais obrigações legais, devendo o poder público, na forma das autoridades competentes, sobretudo o Ministério da Cidadania e as empresas públicas Caixa Econômica e Dataprev, disponibilizar todas as informações referentes ao programa, independentemente de pedidos de acesso, uma vez constatado o interesse público e respeitados os direitos fundamentais em questão (Tavares et al., 2022, p. 33).

No entanto, as autoras destacam que, em contraste com o déficit de transparência ativa nas decisões automatizadas a respeito da gestão de dados, observa-se um uso excessivo e indiscriminado desse princípio no âmbito político. Isso foi evidenciado quando ocorreu a publicação no Portal da Transparência da lista com dados pessoais das/os beneficiárias/os do programa, incluindo seu nome completo, o valor e as parcelas recebidas, além de outros dados sensíveis. Justificada por razões de prestação de contas e prevenção de fraudes, essa abordagem entra em conflito não somente com a própria Lei de Acesso à Informação, que exige a proteção de dados pessoais, mas com os princípios basilares de proteção de dados (Tavares et al., 2022, p. 33). Tal cenário evidencia uma baixa adequação das políticas de proteção social à cultura de proteção de dados e uma negligência à autodeterminação informativa, reconhecida pelo Supremo Tribunal Federal como direito fundamental, uma vez que impede que as pessoas exerçam controle de fato sobre seus dados pessoais vinculados ao programa (Tavares et al., 2022, p. 33).

Um último caso relevante a ser analisado é o do Sistema de Alerta Niñez (SAN) do Chile. De acordo com Valderrama (2021, p. 8), o relatório foi baseado em informações obtidas via solicitação pela Lei de Transparência e uma revisão exaustiva de fontes

secundárias, como materiais da imprensa, apresentações, licitações, propostas técnicas, orientações técnicas, relatórios, contas públicas e ordens de compra do Ministério e outras entidades. No entanto, o autor destaca as dificuldades que se apresentaram no processo investigativo, entre as quais menciona a recusa explícita de figuras-chave do Ministério do Desenvolvimento Social e da Família a serem entrevistadas e a falta de documentação pública sobre o estado atual do instrumento preditivo SAN, que já estava sendo implementado nas OLN (Valderrama, 2021, p. 8).

Considerações sobre proteção de dados pessoais

Dado que as tecnologias de IA estudadas dependem do manejo de grandes quantidades de dados, é essencial discutir as considerações de proteção de dados pessoais identificadas pelas pesquisas. Embora em alguns casos a falta de conformidade com os critérios de proteção de dados pessoais seja evidente, em outros, mesmo que o Estado forneça certas garantias aos indivíduos, os estudos destacam a necessidade de uma supervisão rigorosa para assegurar a proteção declarada.

No Chile, o Sistema Alerta Niñez suscita preocupações específicas sobre o manuseio de dados pessoais de crianças e adolescentes, considerados sensíveis pelo Conselho para a Transparência (CPLT). De acordo com o CPLT, os dados de crianças e adolescentes exigem maior proteção devido à falta de consentimento informado explícito e ao fato de que essas pessoas podem estar menos cientes dos riscos do processamento de seus dados. Portanto, o Conselho limitou a entrega de informações sobre pessoas com menos de 18 anos aos casos nos quais possui autorização do pai, mãe ou tutor/a. Em outros casos, é negada a disponibilização de dados, a fim de evitar danos prováveis e específicos à intimidade das/os crianças e adolescentes (Valderrama, 2021, p. 14-15). O CPLT também questionou acordos, como o convênio entre o Serviço Nacional de Menores e a Agência Nacional de Inteligência, por não se adequarem à proteção dos dados das crianças e adolescentes. Tal posicionamento se dá em conformidade com a Convenção sobre os Direitos da Criança, a qual proíbe ingerências arbitrárias na vida privada das/os pessoas com menos de 18 anos, e consagra o princípio do melhor interesse da criança e do adolescente. A partir dessas diretrizes, segundo uma especialista consultada, entende-se que os dados pessoais dos indivíduos com menos de 18 anos tratados no sistema educacional não devem ser considerados fontes de acesso público (Valderrama, 2021, p. 14-15).

Na Colômbia, o sistema PretorIA, desenvolvido pelo Tribunal Constitucional, automatiza a seleção de processos de tutela para revisão, sem tratar dados pessoais sensíveis,

segundo os autores Saavedra e Upegui (2021, p. 47). Esse sistema opera com textos de sentenças judiciais e não introduz mudanças no acesso ou tratamento dos dados pessoais, pois o processo tradicional (não automatizado) supõe também a remissão dos documentos judiciais. O Tribunal assegurou que o funcionamento do sistema não depende de nomes ou dados específicos e pode operar a partir de informações anônimas. Além disso, a Lei N° 1581 de 2012 estabelece exceções ao consentimento para o processamento de dados necessários para funções judiciais. Apesar disso, embora o sistema não introduza mudanças no acesso e no processamento de dados pessoais, nem afete diretamente os direitos subjetivos, seu impacto social é significativo, uma vez que processos judiciais requerem legitimidade e confiança pública. Por esse motivo, os autores destacam a necessidade de uma rigorosa supervisão técnica e operacional para evitar falhas no funcionamento do sistema e garantir a transparência e a legitimidade do processo (Saavedra e Upegui, 2021, p. 47).

No Uruguai, o sistema Coronavirus UY centralizou os dados pessoais de pacientes, como idade, número de telefone, número da carteira de identidade, sintomas e doenças preexistentes. Essas informações foram organizadas em um único banco de dados, acessível ao Ministério da Saúde Pública (MSP) e aos prestadores de serviços de saúde, que as utilizaram para o acompanhamento de pacientes. O banco de dados centralizado estava sob a propriedade do MSP, responsável por estabelecer diretrizes e protocolos para o seu uso (Yael, 2021, p. 17). Os dados pessoais usados pelo aplicativo são protegidos pela legislação local relativa à proteção de dados pessoais (Lei N° 18.331). Essa norma estabelece que os dados de saúde são sensíveis (art. 4) e, segundo os artigos 17 e 19, eles só podem ser processados por estabelecimentos de saúde e para fins diretamente relacionados ao interesse legítimo da/do remetente e da/do destinatária/o, com o consentimento prévio da pessoa em questão. No entanto, no mesmo dia do lançamento do aplicativo, 20 de março de 2020, a Unidade de Regulamentação e Controle de Dados Pessoais (URCDP) emitiu um parecer (Parecer N° 2/020) que estabeleceu que, devido ao estado de emergência sanitária e à habilitação legal, o processamento de dados de saúde como os coletados pelo aplicativo Coronavirus UY poderia ser realizado sem o consentimento prévio de titulares. Ou seja, o MSP desempenhou uma função de auditoria e supervisão no ecossistema de dados. Esse é um exemplo do uso excessivo de dados sensíveis pelo Estado durante a pandemia, com um alto risco de violação de direitos.

Problemas no uso automatizado de dados e algoritmos

É pertinente analisar a potencial violação de direitos que pode advir da forma como são construídas tecnologias, especialmente algoritmos e sistemas baseados em IA, assim

como os dados usados para o seu treinamento e processamento. Um exemplo relevante para essa análise é o caso do Sistema Alerta Niñez, implementado no Chile.

Segundo Valderrama (2021, p. 31), para modelar o algoritmo do SAN, foram usados dados principalmente de pessoas que interagiram com os serviços estatais de educação e assistência social, que tendem a ter renda e níveis educacionais mais baixos. Isso pode levar a disparidades de acordo com o nível socioeconômico, fazendo com que o modelo tenha uma menor capacidade de identificar crianças de alto risco em um nível socioeconômico mais alto e, ao mesmo tempo, poderia aumentar o risco estimado para famílias de nível socioeconômico mais baixo (Valderrama, 2021, p. 36). Portanto, é fundamental considerar a representatividade dos dados e buscar formas de incluir informações mais amplas e diversificadas para melhorar a precisão e a equidade do sistema preditivo e, dessa forma, fortalecer o funcionamento da política pública na qual é fundamentada sua operação.

Outra questão diz respeito ao Auxílio Emergencial, implementado pelo governo federal do Brasil. O estudo de caso se baseia no uso intensivo de dados para a seleção automatizada de pessoas beneficiárias. Essa infraestrutura de dados é feita com o cruzamento de 34 bancos de dados diferentes, incluindo registros do CadÚnico, do Cadastro Nacional de Informações Sociais (CNIS) e de diversos órgãos governamentais, como o Ministério da Economia e a Caixa Econômica Federal. Todavia, sérias limitações são enfrentadas devido à obsolescência dos registros (Tavares et al., 2022, p. 31). Em particular, foi identificado que os principais bancos de dados, como a Relação Anual de Informações Sociais (RAIS), não são atualizados com informações recentes, afetando negativamente as pessoas que perderam seus empregos e sofreram mudanças em seu status empregatício desde o ano-base de 2018. Essa falha na atualização dos registros resultou na exclusão de pessoas que, apesar de atenderem aos critérios de elegibilidade, não conseguiram acessar o benefício. Desse modo, a arquitetura digital do programa, ao invés de facilitar a inclusão social, reforça barreiras de acesso e limita a eficácia da política de proteção social. Como será discutido posteriormente, essa situação levou à judicialização do programa, o que permitiu uma avaliação detalhada de seu funcionamento.

Em relação ao Sistema Preditivo do Crime Urbano no Chile, é pertinente questionar os efeitos do reforço de vieses, não apenas em termos de vigilância excessiva de determinados espaços e zonas, mas também em relação a como a implementação de tecnologias baseadas nesses vieses pode perpetuar práticas discriminatórias ao concentrar a vigilância em áreas previamente classificadas como conflitivas. Segundo Buschmann (2021, p. 41), o Sistema Preditivo do Crime Urbano é sobretudo alimentado

por duas fontes de dados: casos policiais, que incluem detenções e denúncias relacionadas a delitos de maior conotação social (DMCS) e informações coletadas por meio da plataforma AUPOL usada pela Carabineros. Esses dados incluem dados pessoais das pessoas afetadas, testemunhas e denunciantes, como nome, número de identificação nacional, profissão, gênero e endereço. No entanto, a geração desses dados não é um processo neutro. Como analisa Buschmann (2021, p. 41), cada dado envolve uma cadeia social de produção que pode incorporar vieses e perspectivas contextuais. Isso significa que o banco de dados pode ser composto de registros de situações irregulares e imprecisas, como detenções arbitrárias ou denúncias não investigadas, resultando em um sistema tendencioso que reproduz práticas discriminatórias, especialmente na aplicação de controles de identidade preventivos. Além disso, a pesquisa revelou uma falta de protocolos de avaliação e auditoria externa na coleta de dados (Buschmann, 2021, p. 7).

Contrapesos democráticos: o papel dos órgãos de controle e da justiça

Vale a pena indagar sobre o papel dos órgãos de controle que podem equilibrar a balança a favor da proteção de direitos, principalmente as defensorias públicas e as unidades de auditoria externa, como órgãos oficiais com funções de controle externo sobre a gestão do governo. Por outro lado, também analisaremos o papel que o sistema de justiça desempenhou em alguns dos casos como espaço de denúncia por parte da população para corrigir problemas ligados às falhas nas políticas analisadas, em parte causadas pelo processamento inadequado de dados.

O caso do Boti na cidade de Buenos Aires é um bom exemplo disso. Como Ferreyra relata no seu estudo sobre o chatbot do governo (2024, p. 20), durante 2022, a Auditoria Geral da Cidade de Buenos Aires (AGCBA) –órgão público de controle externo –realizou uma análise exaustiva dos sistemas, processos e tecnologias que garantem a operacionalidade do chatbot Boti, abrangendo o ano de 2021. O relatório de auditoria, publicado em março de 2023,⁷ reconheceu o processo de modernização realizado pelo governo da cidade para facilitar o acesso às informações para o gerenciamento de procedimentos e consultas, mas também as áreas críticas que exigem melhorias, especialmente na formalização de procedimentos administrativos relacionados ao chatbot. O parecer da auditoria destacou a necessidade de estabelecer políticas informáticas robustas para o gerenciamento e a proteção de dados pessoais, bem como

7 Disponível em: https://www.agcba.gov.ar/docs/inf-20230322_2202---CHATBOT-BOTI..pdf (acessado em novembro 2024).

a importância de uma governança eficaz em relação às tecnologias da informação e comunicação. A auditoria também apontou que o gerenciamento e o armazenamento de grandes volumes de dados exigem uma revisão constante das políticas de garantia de segurança e proteção de dados.

Em relação a esse mesmo caso, podemos citar mais um exemplo. Em 2022, a Defensoria Pública da Cidade de Buenos Aires, autoridade de proteção de dados pessoais da cidade, conduziu pesquisa em resposta a uma denúncia sobre o funcionamento do chatbot Boti (Ferreyra, 2024, p. 21). A denúncia, feita por uma cidadã, foi baseada em preocupação com a falta de disponibilidade de termos de uso no acessar ao assistente virtual Boti por meio do site oficial do governo portenho, além de apontar que, com o chatbot, qualquer pessoa que saiba o registro de identidade (DNI) e o número de telefone de outra poderia obter seus dados sensíveis, como resultados de testes de COVID-19. Com base nessas constatações, a Defensoria Pública emitiu recomendações para melhorar a transparência e a integridade dos termos de uso, assim como a inscrição de todos os bancos de dados que contenham dados pessoais no registro correspondente. A necessidade de um tratamento ético e seguro de dados pessoais foi enfatizada, destacando a importância da conformidade com as normas de proteção de dados.

O sistema judiciário desempenhou um papel crucial como intermediário entre a população e o governo para garantir o exercício de direitos. Diante dos problemas observados no âmbito do Auxílio Emergencial no Brasil, e devido à ausência de mecanismos administrativos para revisar decisões automatizadas, o processo judicial se tornou o principal recurso para questionar tais decisões e solicitar uma análise humana na concessão do benefício. Como se trata de um programa federal, a contestação legal foi ajuizada perante à Justiça Federal (Tavares et al., 2022, p. 37). A judicialização do programa se intensificou devido à desatualização dos registros nos sistemas do governo federal. Há casos de pessoas desempregadas que, apesar de não terem emprego formal, apareceram com um vínculo empregatício atual nos bancos de dados, o que as impediu de acessar o benefício. Essa situação levou a um aumento significativo no número de ações judiciais envolvendo o Auxílio, o qual chegou a 76.000 em setembro de 2020 (Tavares et al., 2022, p. 22). Para lidar com a questão, foi estabelecido um convênio entre a Defensoria Pública Federal e o Ministério da Cidadania, o qual permitia que a Defensoria acessasse um sistema específico da Dataprev para a consulta e apresentação de impugnações administrativas (Tavares et al., 2022, p. 22). Dessa forma, argumentam as autoras, é possível considerar que a falta de revisão humana das decisões automatizadas promoveu a judicialização da política, além de ter evidenciado as limitações do

sistema para garantir um acesso inclusivo ao Auxílio Emergencial (Tavares et al., 2022, p. 31).

Sobre esse ponto, Buschmann (2021, p. 9) analisa o papel da Controladoria Geral da República (CGR), uma instituição fundamental no Chile para a transparência e o controle público. Esse órgão autônomo supervisiona o investimento orçamentário de diversas entidades estatais, incluindo a polícia, objeto do estudo de caso. Durante a análise de prestações de contas, a Controladoria pode formular dúvidas e observações, verificando a legalidade de atos mediante auditorias que avaliam atividades, resultados e processos em relação a normas e princípios vigentes. Segundo a autora, essas auditorias incluem controle de orçamento, de legalidade, de gestão, de resultados, de prestação de contas e de avaliação do controle interno. Esse modo de operação da Controladoria a permitiu identificar problemas associados às plataformas digitais utilizadas pela Carabineros a partir de auditorias analisadas no âmbito da análise aqui referida (Buschmann, 2021, p. 9).

A função dos órgãos de controle e supervisão é um exemplo significativo de como o Estado, dentro da estrutura de seu funcionamento democrático, pode mitigar as falhas identificadas nas análises desta seção. Esses órgãos intervieram em casos de violações relacionadas à proteção de dados pessoais, acesso à informação e problemas decorrentes de bancos de dados desatualizados e, em última análise, inadequados para a automação de processos. No entanto, é fundamental destacar a importância de conduzir avaliações de impacto prévias e garantir que a implementação das tecnologias de IA respeite os marcos de direitos humanos, evitando assim situações em que os direitos já terão sido violados previamente à intervenção dos órgãos de controle.

CONCLUSÕES

No âmbito do projeto *Inteligência Artificial e Inclusão*, dez casos de uso de tecnologias, em 7 países da América Latina, foram analisados em um período de quase 6 anos. Durante esse período, entre 2019 e 2024, o desenvolvimento de tecnologias baseadas em IA aumentou consideravelmente, assim como difundiu-se seu uso, principalmente a partir da massificação do uso de IA generativa no final de 2022. Além disso, durante esse período, a pandemia de COVID-19 começou e terminou, correspondendo a situação excepcional que intensificou o uso da tecnologia como ferramenta para a gestão de procedimentos e serviços, mas também de políticas fundamentais de seguridade social. Esse período também foi marcado pelo lançamento de alguns dos marcos éticos e regulatórios mais influentes na região, como os Princípios da OCDE para

uma IA Confiável (2019),⁸ a Recomendação sobre a Ética da Inteligência Artificial da UNESCO (2021)⁹ e a Lei de Inteligência Artificial da União Europeia (2024).¹⁰ A seguir, analisaremos quais fatores se mantêm e o que mudou com relação ao uso da IA no Estado durante esse espaço temporal.

A primeira observação tem relação com a persistente falta de marcos regulatórios adequados para a implementação dessas tecnologias. Os dados do primeiro relatório do Índice Global de Inteligência Artificial Responsável, publicado em 2024, ilustram esse ponto. Em relação às dimensões de ações e estruturas de governança, as quais estão baseadas na análise da existência de estratégias nacionais de IA, avaliações de impacto nos direitos, ações para revisão humana, considerações de proporcionalidade, diretrizes específicas de transparência e explicabilidade, apenas dois países da região excederam 50% da pontuação. Na dimensão de direitos humanos e IA, nenhum dos países obteve pontuação superior a 50%. Essa dimensão de análise inclui indicadores sobre equidade de gênero, proteção de dados e privacidade, participação pública, direitos das crianças e adolescentes, proteção trabalhista, entre outros.¹¹ Essa ausência de marcos regulatórios específicos para o uso da IA no Estado já era uma das conclusões do primeiro relatório comparativo publicado no âmbito deste projeto (Velasco e Venturini, 2021) – e, para este artigo, se mantém.

Na área de proteção e uso de dados pessoais, os órgãos de controle desempenharam um papel fundamental para evitar que o processamento automatizado de dados violasse direitos fundamentais, como o acesso a benefícios sociais. Um exemplo é o caso do Auxílio Emergencial no Brasil, onde as deficiências na atualização dos bancos de dados causaram danos significativos às pessoas que tentaram acessar o programa. O caso evidencia os riscos associados às políticas baseadas no processamento automatizado de dados e denota a importância de garantir a qualidade dos dados que serão processados por algoritmos.

Sobre o acesso a informações públicas, há problemas persistentes, que atravessaram estudos de casos durante todo o período de sua condução. Respostas incompletas a pedidos de acesso à informação, como aconteceu com o chatbot Boti na cidade

8 Disponível em: <https://oecd.ai/en/ai-principles>.

9 Disponível em: <https://www.unesco.org/es/legal-affairs/recommendation-ethics-artificial-intelligence>.

10 Mais informações em: <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>.

11 O relatório completo está disponível em: <https://www.global-index.ai/Region-South-and-Central-America>.

de Buenos Aires, ou recusas explícitas para conceder entrevista, como na análise do Sistema Alerta Niñez no Chile, são exemplos que ilustram as dificuldades de pesquisar o uso de Inteligência Artificial pelo Estado. A falta de transparência, entretanto, não é o único desafio. Há também uma questão envolvendo a publicação de informações em desacordo com a proteção de dados pessoais, como evidenciado no Auxílio Emergencial no Brasil. Nesse caso, uma lista com dados pessoais das pessoas beneficiárias do programa foi publicada no Portal da Transparência. Embora essa ação tenha sido justificada sob o argumento da prestação de contas, como apontam as autoras, ela entra em conflito com a Lei de Acesso à Informação, que exige que as autoridades públicas protejam os dados pessoais e ajam de acordo com seus princípios basilares (Tavares et al., 2022, p. 33). Portanto, é essencial conceber e interpretar marcos regulatórios de forma complementar para garantir que a proteção de direitos fundamentais seja priorizada.

Outro ponto de alerta é a persistente falta de espaços para participação significativa que garantam a diversidade e a inclusão das diversas partes interessadas não apenas na implementação de políticas promovidas pelos diferentes poderes do Estado, mas também nos espaços incipientes de regulação. Em uma pesquisa anterior, a Derechos Digitales analisou os processos participativos gerados no âmbito dos chamados planos e estratégias de Inteligência Artificial promovidos por diferentes governos da região. Essa pesquisa mostra que, embora tenha havido esforços para gerar espaços participativos, os esforços ainda são insuficientes para empoderar a população na tomada de decisões sobre políticas públicas que possam afetar diretamente o exercício de seus direitos (Hernández et al. 2022).

Dessa forma, fica evidente a persistência de problemas relacionados à proteção de dados pessoais, ao acesso à informação pública e à falta de espaços de participação significativa na implementação de tecnologias de Inteligência Artificial pelo Estado. Embora a adesão a marcos éticos seja desejável, ela não é suficiente; é essencial estabelecer regras claras e marcos de governança que garantam a participação das múltiplas partes interessadas. Na Derechos Digitales, consideramos prioritária a incorporação de uma perspectiva de direitos humanos em todos os processos relacionados à regulação da IA, seja por meio de iniciativas do poder Executivo ou dos parlamentos da região, visando promover o uso responsável e inclusivo dessas tecnologias na gestão governamental, que inclua limitações claras.

BIBLIOGRAFIA

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.

Consortio 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>

Ferreira, 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) *Inteligencia 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-urgent-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.

