



Universidade de Brasília

Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas - FACE

Departamento de Gestão de Políticas Públicas - GPP

BRUNA DE MELO XAVIER COSTA

**MAPEAMENTO E ANÁLISE DAS INICIATIVAS DE  
INTELIGÊNCIA ARTIFICIAL NO SETOR PÚBLICO BRASILEIRO:  
potenciais riscos e benefícios a serem oferecidos pela tecnologia  
para a democracia**

Brasília – DF

2023

BRUNA DE MELO XAVIER COSTA

**MAPEAMENTO E ANÁLISE DAS INICIATIVAS DE  
INTELIGÊNCIA ARTIFICIAL NO SETOR PÚBLICO BRASILEIRO:  
potenciais riscos e benefícios a serem oferecidos pela tecnologia  
para a democracia**

Monografia apresentada ao Departamento  
de Gestão de Políticas Públicas como  
requisito parcial à obtenção do título de  
Bacharel em Gestão de Políticas Públicas

Orientadora: Professora Dra. Christiana  
Soares de Freitas

Brasília – DF

2023

## AGRADECIMENTOS

Agradeço a Deus, a minha fonte de força e luz para a superação de todos os obstáculos e desafios da minha jornada. Agradeço e dedico este trabalho, que marca o encerramento de um ciclo, a minha mãe e a meu pai. Expresso minha eterna gratidão por não terem medido esforços em benefício da minha formação intelectual e pessoal, sempre me apoiando e me elevando no que eu precisei com muito amor e carinho.

Ao meu querido namorado, Thaiyan, por reconhecer e compreender meus momentos de estresse, impaciência e cansaço, oferecendo suporte que me acalentou e amenizou todos os momentos difíceis. Mais que tudo, agradeço por quem você é. Esta é apenas uma das conquistas que quero viver ao seu lado.

Aos professores e professoras da UnB, com quem tive a honra de aprender além de materiais didáticos e cujas aulas contribuíram para meu desenvolvimento acadêmico, profissional e humano. Destaco primeiramente minha sincera gratidão à Professora Christiana de Freitas pela dedicação e leveza na orientação deste trabalho, e por ser minha fonte de inspiração no meio acadêmico. Agradeço ao Professor Marcos Urupá por ter aceitado o convite para compor a Banca e pelos ricos comentários que ajudaram a elevar o nível da minha pesquisa. Agradeço ao Professor Pedro Zuchi, do Departamento de Economia, com quem tive o privilégio de colaborar e aprender muito durante minha passagem pela coordenação da Monitoria de Introdução à Economia. Agradeço também à Professora Marina Moreira, do Departamento de Administração, por ter me introduzido tão energeticamente à área que considero mais empolgante na Gestão Pública, a de Inovação. Reservo agradecimento especial à Professora Sheila Tolentino, que me auxiliou muito no processo de elaboração do meu projeto de pesquisa. Seus ensinamentos contribuíram para que eu me tornasse uma pesquisadora melhor.

Aos colegas que fiz ao longo da minha jornada pela UnB no curso de GPP e na Monitoria de Introdução à Economia, na qual vivi momentos incríveis e enriquecedores. À minha amiga e irmãzinha do coração, Ana Beatriz, por todo o apoio emocional durante a elaboração da pesquisa. À Julia Louise, minha principal companheira no curso, que me alegrou ao longo do curso e me acolheu nos dias difíceis, e foi a pessoa certa para fazer os inúmeros trabalhos em dupla comigo.

## RESUMO

A Inteligência Artificial (IA) é uma tecnologia emergente que vem conduzindo mudanças críticas na sociedade vigente. À vista das funcionalidades desse instrumento, o interesse pela IA passou por avanços acelerados nos últimos cinco anos no setor público. Tendo em vista sua capacidade de analisar grandes volumes de dados de forma mais rápida do que os humanos, bem como de fornecer sugestões sobre como otimizar os serviços públicos e aproximar os governantes dos governados, o uso de IA pela gestão pública brasileira vem crescendo como instrumento capaz de aumentar a eficiência da máquina pública. Apesar de suas inúmeras potencialidades, trata-se de uma tecnologia que pode apresentar riscos à democracia a partir da reprodução de comportamentos discriminatórios provenientes de algoritmos, efeito relacionado a aspectos técnico-científicos inerentes ao atual estado da arte desse tipo de artefato. Tal fator é ainda mais alarmante quando aplicado à área de Segurança Pública. Questiona-se, assim, quais as iniciativas de IA sendo usadas na gestão pública para a área de segurança pública em nível federal e na sociedade civil no Brasil até setembro de 2023. A partir disso, pretende-se investigar os potenciais riscos e benefícios a serem oferecidos pela tecnologia à democracia. A pesquisa desenvolvida é do tipo exploratória e descritiva, com abordagem mista. Para análise das iniciativas, utilizou-se dados primários e secundários, além de pesquisa bibliográfica e documental. Foi possível encontrar treze (13) iniciativas do governo federal e uma da sociedade civil. Identificou-se, além do problema da opacidade algorítmica, uma opacidade na gestão. Averiguou-se que as ferramentas de IA contribuem para aumento de eficiência na gestão pública sob a ótica dos órgãos implementadores. Contudo, foi possível apontar potenciais impactos negativos a direitos para todas as ferramentas. Verificou-se que nem todas as ações para mitigar os possíveis riscos a direitos estão sendo realizadas pela gestão pública. Conclui-se que, para a manutenção da democracia, a eficiência na gestão pública possibilitada pela inteligência artificial não pode ser alcançada às custas dos direitos fundamentais.

**Palavras-chave:** inteligência artificial, gestão pública, democracia, segurança pública, eficiência na gestão pública, riscos e benefícios à democracia.

## ABSTRACT

Artificial Intelligence (AI) is an emerging technology that has been driving critical changes in the current society. Given the functionalities of this instrument, interest in AI has undergone accelerated advances in the last five years in the public sector. Given its ability to analyze large volumes of data faster than humans, as well as to provide suggestions on how to optimize public services and bring rulers closer to the governed, the use of AI by Brazilian public management has been growing as an instrument capable of increasing the efficiency of the public machine. Despite its countless potentialities, it is a technology that can present risks to democracy through the reproduction of discriminatory behaviors arising from algorithms, an effect related to technical-scientific aspects inherent to the current state of the art of this type of artifact. This factor is even more alarming when applied to the area of Public Security. The question is, therefore, which AI initiatives are being used in public management for the area of public security at the federal level and in civil society in Brazil until September 2023. From this, we intend to investigate the potential risks and benefits to be offered by technology to democracy. The research developed is exploratory and descriptive, with a mixed approach. To analyze the initiatives, primary and secondary data were used, in addition to bibliographic and documentary research. As a result, it was possible to find thirteen (13) initiatives from the federal government and one from civil society. In addition to the problem of algorithmic opacity arising from the lack of transparency of AI systems, an opacity in public management was identified. It was found that AI tools, in general, contribute to increasing efficiency in public management from the perspective of implementing bodies. However, it was possible to point out potential negative impacts on rights for all tools. It was found that not all actions to mitigate possible risks to rights are being carried out by the public management. It is concluded that, for the maintenance of democracy, the efficiency in public management made possible by artificial intelligence cannot be achieved at the expense of fundamental rights.

**Keywords:** artificial intelligence, public management, democracy, public security, efficiency in public management, risks and benefits to democracy.

## LISTA DE FIGURAS

<b>Figura 1</b> - Número de textos com palavras-chave relacionadas à IA publicados na base Scopus por ano .....	43
---	----

## LISTA DE TABELAS

<b>Tabela 1</b> - Métodos utilizados e órgãos implementadores para cada iniciativa mapeada .....	50
<b>Tabela 2</b> - Capacidade da ferramenta de IA de promover eficiência a partir da perspectiva dos órgãos implementadores e/ou desenvolvedores .....	76
<b>Tabela 3</b> - Direitos fundamentais a serem impactados pelo uso das iniciativas da gestão pública que utilizam recursos de IA .....	81

## SUMÁRIO

1. Introdução .....	10
1.1 Contextualização do tema .....	10
1.2 Pergunta de pesquisa .....	12
1.3 Objetivos.....	14
1.3.1 Objetivo geral .....	14
1.3.2 Objetivos Específicos .....	15
2 Referencial Teórico .....	18
2.1 Democracia e o Uso de Tecnologias .....	18
2.1.1 Democracia, Tecnologias e Eficiência na Gestão Pública .....	22
2.1.2 Democracia Participativa e Tecnologias aplicadas à Gestão Pública .....	25
2.2 Inovações Tecnológicas na Gestão Pública .....	28
2.2.1 Inteligência Artificial.....	30
2.2.2 IA na Gestão Pública.....	33
2.2.3 Uso de recursos de IA na Segurança Pública .....	38
3 Metodologia.....	43
3.1 Caracterização da pesquisa .....	43
3.2 Procedimentos de coleta dos dados da pesquisa.....	44
3.3 A amostra .....	46
3.4 Instrumentos de coleta e análise de dados.....	47
4 Análise dos Dados Coletados .....	50
4.1 Descrição e caracterização de iniciativas de IA do Governo Federal orientadas para Segurança Pública .....	50
4.2 Iniciativa da Sociedade Civil em Parceria com o Governo Federal .....	67
4.3 Uso de ferramentas de IA e aumento de eficiência na gestão pública .....	68
4.3.1 Apresentação do desempenho e/ou dos resultados alcançados pelas ferramentas baseadas em IA utilizadas na Gestão Pública .....	70

4.3.2 Análise da eficiência das ferramentas de IA com base na visão do órgão implementador/desenvolvedor .....	75
4.4 Riscos democráticos que envolvem o uso de IA na gestão pública .....	80
4.5 Atuação do MCTI no monitoramento das ferramentas de IA voltadas para a área de Segurança Pública.....	91
4.6 Limitações da Pesquisa e Agenda de Estudos Futuros.....	92
5 Considerações Finais .....	95
6 Referências .....	100
Apêndices.....	107
APÊNDICE A – QUESTIONÁRIO ENVIADO AO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO .....	107
APÊNDICE B - QUESTIONÁRIO ENVIADO AO INSTITUTO GLÓRIA .....	108

## 1. Introdução

A presente seção está segmentada nos seguintes tópicos: contextualização, problema de pesquisa, objetivo geral, objetivos específicos e justificativa. Essa divisão objetiva dispor como a pesquisa foi concebida.

### 1.1 Contextualização do tema

Tecnologias inovadoras têm sido aplicadas em diversos setores da sociedade, e a Inteligência Artificial (IA) tem se destacado como uma dessas tecnologias emergentes que vem conduzindo mudanças críticas na sociedade vigente. A IA busca replicar a capacidade humana, permitindo a execução autônoma e ágil de atividades como o raciocínio lógico, a interpretação, a comunicação e o aprendizado por meio de dispositivos gerados em um desempenho aprimorado nas tarefas para as quais foram criadas (SAVÉRIO & NICOLAS, 2022).

Campos e Figueiredo (2022) indicam que o crescimento da IA nos últimos anos foi impulsionado por fatores como o desenvolvimento das estatísticas e métodos probabilísticos, pelo aumento da disponibilidade do número de dados e pelo aumento da eficiência da capacidade computacional. Tal recurso, por ter desenvolvimento recente, ainda tem muito potencial para ser explorado. Conseqüentemente, há muitas incertezas e desconfianças acerca das suas funcionalidades e dos riscos a partir dos impactos que essa tecnologia pode gerar na sociedade.

Segundo a Organização para Cooperação e Desenvolvimento Econômico (OCDE), a IA é uma ferramenta poderosa com grande potencial para proporcionar bem-estar para a população, contribuir para uma atividade econômica global sustentável, impulsionar a inovação e a produtividade, além de auxiliar no enfrentamento dos desafios globais vigentes (OCDE, 2019). Já é possível visualizar os impactos da Inteligência Artificial sobre inúmeros setores da vida humana, com alteração dos paradigmas atuais da produção industrial, das relações pessoais e do cuidado com a vida (BRASIL, 2021b). Devido ao seu caráter transversal, a IA possibilita o desenvolvimento de soluções inovadoras que permitem enfrentar uma

ampla gama de problemas, resultando em melhorias socioeconômicas significativas para a sociedade (CÓBE, et al., 2020).

À vista das potencialidades desse instrumento, o interesse pela Inteligência Artificial vem crescendo de forma acelerada nos últimos cinco anos não apenas no setor privado, mas também no setor público. Nesse sentido, tal tecnologia apresenta enorme potencial para os governos, uma vez que é capaz de analisar grandes volumes de dados de forma mais rápida do que os humanos, de identificar ideias e tendências, bem como de fornecer sugestões sobre como otimizar os serviços públicos (WILNER, 2018). Em razão disso, diversas nações vêm adotando a IA como ferramenta nos órgãos públicos para transformar processos físicos em digitais e promover a personalização de serviços públicos destinados a melhorar a relação entre os governos e os cidadãos.

Estimativa de riscos com base em dados, segurança cibernética, segurança doméstica, vigilância e monitoramento de fronteiras, previsão de policiamento, reconhecimento facial, detecção automatizada de fraudes, assistência médica, triagem de pacientes, auxílio jurídico, transporte, processamento de linguagem natural, relações públicas, modelos preditivos, planejamento urbano, entre outros, são exemplos de como a inteligência artificial vêm sendo aplicada nos diferentes governos mundiais para atender às demandas sociais e buscar melhorar a oferta de serviços públicos.

Apesar de suas inúmeras funcionalidades, trata-se de uma tecnologia muito recente que, por consequência, gera muitas dúvidas sobre suas funcionalidades e os impactos que essa pode gerar no mundo. Dessa forma, diversos governos e até mesmo órgãos internacionais buscaram definir diretrizes para o desenvolvimento e aplicação da IA. No Brasil, tal discussão ainda é bastante recente. Em 2018, a Estratégia Brasileira para a Transformação Digital (E-Digital) definiu a Inteligência Artificial como tema prioritário em virtude de seus impactos transversais sobre o país. No entanto, a matéria passou a obter mais centralidade nos planos governamentais a partir da elaboração da *“Recomendação do Conselho da OCDE sobre IA”*, documento publicado pela OCDE, em 2019. Assim, em 2020 o Ministério da Ciência, Tecnologia e Inovação (MCTI), ao definir como prioridade a área de Inteligência Artificial, no que se refere a projetos de pesquisa, de desenvolvimento de tecnologias e inovações, para o período 2020 a 2023, elaborou a Estratégia Brasileira de Inteligência Artificial – EBIA.

A tendência no Brasil e em todo o mundo é que haja um crescimento do uso de IA pelo poder público. Isso fica perceptível na EBIA, visto que duas de suas nove ações estratégicas referem-se a diretrizes para seu desenvolvimento e aplicação no poder público e na segurança pública. O documento aponta que a modernização dos processos administrativos e operacionais, que pode ser promovida pela IA como inovação tecnológica aplicada ao setor público, possibilita que o Estado supere obstáculos burocráticos e restrições orçamentárias para oferecer serviços novos, melhores e mais eficientes à população (BRASIL, 2021). Assim, o uso de IA pelo governo brasileiro conta com perspectivas de grandes benefícios, mas ainda enfrenta desafios consideráveis, como barreiras à inovação no setor público, riscos éticos e necessidade de formulação das devidas medidas regulatórias (DA SILVA, SILVA, DA SILVA RABÊLO, 2021).

Tendo em consideração o crescente interesse mundial e nacional na utilização da Inteligência Artificial, e os potenciais riscos e benefícios da aplicação dessa tecnologia dentro do serviço público no Brasil, propõe-se que seja realizado um estudo para mapear as principais iniciativas de Inteligência Artificial e seus casos de uso no governo executivo federal brasileiro, bem como investigar quais são esses riscos e benefícios à democracia que as aplicações de IA podem trazer.

## **1.2 Pergunta de pesquisa**

A administração pública enfrenta diariamente o desafio de identificar os problemas públicos e trabalhar na estruturação das opções de soluções e resultados. Nesse ínterim, o problema público é a base de toda identificação e caracterização de determinada política pública e está interligado às demandas da sociedade (CAPELLA, 2018). A partir do diagnóstico de cada problema público, os tomadores de decisão optam por estabelecer ou não estabelecer ações para enfrentá-los, sendo tal escolha a política pública (DYE, 2005).

Os estudos de March e Simon (1967), conforme apresentados por Pereira, Lobler e Simonetto (2010), demonstram que, dadas as limitações de tempo e de conhecimento sobre todas as informações e dados disponíveis, o homem é desprovido da capacidade de tomar uma decisão ideal, se contentando com o satisfatório em detrimento do ótimo. Nesse sentido, apesar dos governos possuírem

um gigantesco volume de dados armazenados das interações com seus cidadãos, a capacidade humana não permite avaliar todos os dados fornecidos, principalmente para interpretar tendências ou comportamentos. Com o desenvolvimento de tecnologias como a Inteligência Artificial, é possível que soluções tecnológicas criem condições para armazenar, tratar e interpretar esses grandes volumes de dados (CAMPOS; FIGUEIREDO, 2021).

Nessa perspectiva, é notório que a Inteligência Artificial é uma inovação tecnológica com aplicações aparentemente infundáveis, que, em geral, podem ser utilizadas no setor público para automatizar ou auxiliar na tomada de decisão (VEALE; BRASS, 2019; VAN NOORDT; MISURACA, 2022). Suas funcionalidades podem fornecer maior suporte à administração pública para utilizar com maior eficiência os dados sob sua tutela na resolução de problemas (CAMPOS; FIGUEIREDO, 2021). Sendo assim, é possível que sua aplicação seja utilizada para definir diretrizes e ações para enfrentamento de determinado problema da sociedade, tornando-se uma ferramenta interessante e poderosa no arsenal de um gestor público.

Segundo a visão de Freitas, Sampaio e Avelino (2022), as inovações tecnológicas podem ser utilizadas para gerar melhorias à democracia para além da questão de participação popular. Para os autores, o uso da tecnologia pode auxiliar o Estado na oferta de serviços públicos cada vez mais eficientes, de modo a atender às demandas dos cidadãos e, assim, viabilizar o fortalecimento democrático (FREITAS, SAMPAIO, AVELINO, 2022). Nessa perspectiva, a utilização de IA pelo poder público pode gerar benefícios à democracia ao passo que gera transformações capazes de apoiar com maior conjunto de dados os processos decisórios, além de otimizar processos operacionais, reduzindo prazos e fornecendo respostas mais eficazes aos problemas públicos encontrados (BRASIL, 2021b).

Concomitantemente, a utilização da IA e algoritmos pela gestão pública pode ter consequências negativas para a democracia. De Araujo, Zullo e Torres (2020) e Fornasier (2021) indicam que o processo decisório dos algoritmos pode reproduzir desigualdades, efeito relacionado a aspectos técnico-científicos inerentes ao atual estado da arte desse tipo de artefato. A exemplificar, ações policiais e decisões judiciais no contexto criminal, fundamentadas em processos cognitivos algorítmicos com tendências discriminatórias, têm o potencial de violar a dignidade da pessoa humana, o direito à igualdade e a liberdade dos cidadãos, resultando em prejuízos para regimes democráticos (DE ARAUJO, ZULLO, TORRES, 2020). Dessa forma, o

Estado, ao utilizar IA sem medidas regulatórias e instruções de governança bem definidas, pode incorporar em seu aparato institucional medidas nocivas à democracia derivadas do mau uso intencional ou não intencional da tecnologia.

Na área de segurança pública, que será o foco das iniciativas analisadas, a IA pode apresentar sérios problemas associados a viés e discriminação decorrentes, em sua maioria, de bases de dados de treinamento insuficientemente representativas e, portanto, inadequadas para fazer generalizações (BRASIL, 2020). O uso de Sistemas de Reconhecimentos Faciais (SRF) para fins de vigilância pública já é uma tendência mundo afora para identificar indivíduos foragidos ou comportamentos criminosos em locais públicos.

Contudo, erros em SRF utilizados para segurança pública podem representar constrangimentos, prisões arbitrárias e violações de direitos fundamentais, como o princípio da não discriminação e da presunção de inocência, sendo extremamente prejudiciais para a democracia (BRASIL, 2021b). A tendenciosidade prejudicialmente discriminatória também pode surgir no processo de amostragem para classificação. Por exemplo, ao coletar dados sobre a incidência de crimes, é possível que a polícia tenha detido de forma desproporcional pessoas com perfil de imigrante no passado, ou de raça negra, ou residentes de determinados bairros da cidade, o que pode resultar em distorções nos dados que refletem preconceitos existentes no sistema (FORNASIER, 2021).

Nesse panorama, a extensão completa dos resultados positivos ou negativos da utilização da IA ainda não é claro no setor público brasileiro, devido à falta de estudos que contemplam o impacto da aplicação dessa ferramenta, bem como à recenticidade da sua aplicação, o que dificulta a compreensão dos seus impactos (KUZIEMSKI; MISURACA, 2020). Dessa forma, o presente estudo busca responder à seguinte pergunta de pesquisa: **quais os benefícios e riscos à democracia observados com a implementação de IA pela gestão pública para a Segurança Pública?**

### **1.3 Objetivos**

#### **1.3.1 Objetivo geral**

Com o propósito de oferecer luz ao problema de pesquisa, este estudo apresenta como objetivo geral identificar, para posterior análise, as iniciativas de IA sendo usadas na gestão pública para a área de segurança pública em nível federal e na sociedade civil no Brasil e, a partir disso, investigar seus potenciais riscos e benefícios à democracia.

### **1.3.2 Objetivos Específicos**

Para alcançar o objetivo geral proposto, a pesquisa seguirá os objetivos específicos descritos a seguir:

1. Identificar as iniciativas para segurança pública, que utilizam recursos de IA, implementadas pelo governo federal até setembro de 2023;
2. Identificar e descrever as iniciativas para segurança pública, que utilizam recursos de IA, implementadas pelas organizações da sociedade civil e comunidade acadêmica até setembro de 2023;
3. Descrever e analisar as iniciativas mapeadas com base em suas características gerais e seus órgãos implementadores;
4. Identificar como os instrumentos de IA mapeados podem contribuir para o aumento da eficiência na gestão pública e proporcionar benefícios democráticos;
5. A partir das iniciativas identificadas, analisar os possíveis riscos do uso dos artefatos de IA à democracia.

### **1.4 Justificativa**

O uso acelerado de Tecnologias da Informação e Comunicação (TICs) afeta não somente a estrutura das sociedades, como também os moldes da Administração Pública. A Estratégia de Governo Digital 2020-2022, regulamentada pelo Decreto nº 10.332/2020, apresenta como um de seus objetivos o desenvolvimento de um Governo Inteligente, que implemente políticas efetivas com base em dados e evidências e que antecipe e solucione, de forma proativa, as necessidades do cidadão

e das organizações. Assim, pressupõe utilizar e integrar os progressos científicos e tecnológicos no campo da ciência de dados e da IA para desenvolver soluções que aprimorem os serviços públicos. Essas soluções são fundamentadas principalmente no conhecimento das realidades e experiências dos cidadãos, em vez de depender exclusivamente de intuições e ideias pré-existentes dos agentes públicos sobre as situações em que é necessário intervir.

Este tema é extremamente complexo devido a sua transversalidade, apresentando diversos impactos em diversas áreas como saúde, transparência, *accountability*, relações públicas, segurança cibernética, mobilidade, planejamento urbano e educação. Para fins deste trabalho, optou-se por destacar uma área específica: a de segurança pública. Tal área torna-se particularmente pertinente a esta temática tendo em vista que envolve a capacidade da IA de aperfeiçoar o sistema de segurança pública, o que pode ser muito positivo em um país tão violento quanto o Brasil. Contudo, o uso de IA para segurança pública pode oferecer riscos e impactos à direitos fundamentais se implementados sem as devidas restrições legais e instruções de governança.

A partir da noção das mudanças críticas que a IA pode fazer na sociedade, a análise realizada nesta pesquisa adquire uma perspectiva crítica mais profunda ao estabelecer uma conexão com a crise atual da democracia liberal, como observada por Castells (2018), conforme será discutida no referencial teórico. Considerando que o uso das TICs permite desde o aumento da proximidade entre os cidadãos e seus governados, até o seu afastamento ou uso para controle da sociedade, este trabalho, ao buscar evidenciar quais os possíveis riscos e benefícios dos artefatos de IA para a democracia no Brasil, contribui para a discussão sobre os possíveis rumos da democracia brasileira.

Ainda existem poucos autores do campo de públicas que refletem acerca das implicações do uso de IA pela gestão pública para o desenvolvimento do Estado brasileiro, o que também torna difícil identificar todas as iniciativas de IA sendo utilizadas na gestão pública. Nesse sentido, o mapeamento que será realizado e a caracterização das iniciativas de IA podem colocar em evidência iniciativas mais desconhecidas que ainda precisam de estudos mais aprofundados nas mais diversas áreas do conhecimento. Desse modo, a presente pesquisa pode funcionar como um guia para futuras pesquisas acadêmicas. O objetivo, aqui, não é esgotar a análise

acerca das ferramentas em todos os seus aspectos, mas oferecer uma avaliação crítica acerca de seus potenciais riscos e benefícios para democracia.

Além disso, a presente pesquisa pode apresentar valor social ao fornecer informações para gestores públicos que possam adotar algumas medidas de IA com alto potencial para gerar aprimoramentos na prestação de serviços públicos como inspiração para seus órgãos, bem como ao apontar os potenciais riscos que precisam ser mitigados no caso de adoção da tecnologia.

## 2 Referencial Teórico

Nesta seção serão abordados alguns conceitos a respeito de democracia, bem como fatores que contribuem para as crises da democracia liberal e como as inovações tecnológicas poderiam contribuir para restaurar a legitimidade do regime. Dentro desta lógica, são investigadas as concepções sobre o conceito de eficiência, como este se relaciona com o uso de tecnologias e com a democracia. Não obstante, será apresentado como as tecnologias podem favorecer ou trazer riscos para a participação cidadã, elemento fulcral das democracias liberais. Em seguida, serão apresentadas as várias definições de inteligência artificial, bem como seus conceitos envolvidos. Por último, trata-se sobre aplicações de inteligência artificial na gestão pública, com espaço dedicado à sua aplicação na área de segurança pública.

### 2.1 Democracia e o Uso de Tecnologias

Definir democracia não é uma tarefa simples. Por se tratar de um conceito histórico, torna-se muito elástico e está longe de ser uma unanimidade na literatura. Com origem na Grécia Antiga, a etimologia da palavra “democracia” provém do grego e seu significado literal é “poder da maioria” (JALOTO & MOREIRA, 2023).

Ao longo do tempo, o conceito foi posto a diversas interpretações. Segundo os autores adeptos à escola schumpeteriana, a democracia é um método político e procedimental, no qual o povo tem a oportunidade de decidir quem vai governá-los e representar seus interesses (O’DONNELL, 1999). Nesta perspectiva, denominada tecnocrata, o sistema democrático é abordado como um arranjo institucional, no qual a participação cidadã pode limitar-se ao voto (ABRUCIO & LOUREIRO, 2018).

Em contrapartida, o teórico da democracia pluralista Robert Dahl compreende que a democracia vai além de aspectos procedimentais; a característica-chave da democracia para o autor refere-se à “contínua responsividade do governo às preferências de seus cidadãos, considerados politicamente iguais” (DAHL, 1997, p. 25). Em outras palavras, o governo democrático deve formular políticas públicas que atendam às preferências e necessidades dos cidadãos, de modo a preservar seus direitos garantidos de forma legítima. Neste sentido, pode-se inferir que a democracia remete ao interesse público e demanda constante deliberação.

Seguindo a perspectiva pluralista de democracia, Dahl (1998) indica que, além da participação igualitária no processo de decisão, a democracia deve envolver como elementos norteadores a existência de certas instituições e procedimentos que garantam a participação igualitária e significativa dos cidadãos. Tais instituições incluem elementos como eleições livres, liberdade de expressão, direitos políticos e civis protegidos, acesso à informação, transparência em suas ações, entre outros. Os procedimentos democráticos são, assim, capazes de fornecer um quadro normativo para a tomada de decisões políticas, garantindo que as preferências e interesses dos cidadãos sejam levados em consideração (ABRUCIO & LOUREIRO, 2018).

Para mais, a democracia compreendida por Robert Dahl deve ir além do simples processo de tomada de decisões. Tal sistema também requer a proteção dos direitos civis e liberdades individuais, bem como a existência de um Estado de direito que limite o poder governamental e garanta a responsividade dos atores políticos por meio de instituições formais (SABL, 2015).

Apesar da abundância de compreensões existentes para democracia, a grande parte da literatura aponta para a crise das democracias liberais na atualidade. Ao destacar as múltiplas crises da atualidade, Castells (2018) revela que a crise das democracias se estende por todo o mundo, embora seja marcada por particularidades locais e se configura como um “colapso gradual de um modelo de representação”. Fatores como a corrupção, o sentimento global de medo proveniente de práticas terroristas, a política midiática, política do escândalo e autonomia comunicativa dos cidadãos, contribuem para a ameaça às democracias liberais (CASTELLS, 2018).

Essa crise também pode ser verificada em índices estatísticos, como os dados dos relatórios *Democracy Index*, produzidos pelo *The Economist Intelligence Unit*. A pontuação média global dos países avaliados no índice caiu de 5,44, em 2018, para sua pior pontuação desde que o índice foi produzido em 2006, chegando a 5,28 em 2021, em parte, devido aos impactos da pandemia do COVID-19, segundo os relatórios (EIU, 2021). O índice apresentou um leve aumento na sua última mensuração, nos anos de 2021 e 2022. Entretanto, o crescimento foi abaixo do previsto pelos especialistas, que especularam o controle da pandemia como um possível motivo para observar um avanço significativo do índice. Esse tímido crescimento foi justificado nas análises do *The Economist Intelligence Unit* por tensões geopolíticas e crises econômicas globais (EIU, 2022).

O relatório *Autocratization Changing Nature?* do *V-Dem Institute*, também indica para o cenário atual de declínio de regimes democráticos no mundo (V-DEM, 2022). O relatório, que utiliza mais de 500 índices e 4.000 avaliadores de todo o mundo para classificar os regimes políticos, revela que o nível de democracia global em 2021 retrocedeu ao que era observado em 1986. Ademais, o número de democracias liberais regrediu para 34 em 2021, valor que não era tão baixo desde 1995. O relatório, ainda, calcula que, pela primeira vez em 20 anos, o número de democracias liberais é menor que o número de regimes ditatoriais. O relatório também ressalta os mecanismos usados por líderes da democracia para corroer o sistema. O cerceamento da liberdade de expressão e de imprensa é o mais abordado. Ademais, os direitos fundamentais estão se deteriorando em 35 países, sendo que há 10 anos eram 7 (V-DEM, 2022).

Warren (2002) argumenta que o ideal democrático foi perdendo forças ao longo dos anos desde seu despertar nos países centrais durante os séculos XIX e XX. Para o autor, isso ocorreu em razão do sufrágio universal passar de uma forma de exercício democrático para assumir o significado da própria democracia. Esse modelo democrático liberal gera desinteresse pela política, ruptura da relação entre governados e governantes, esvaziamento das instituições do sistema político e falta de sentimento público (WARREN, 2002; CASTELLS, 2018).

Tendo em vista os fatores supracitados, a crescente crise na democracia vivenciada nos últimos anos segue corroborando o argumento de que o ideal de democracia representativa baseado apenas no voto é insuficiente para que o Estado possa atender às complexas demandas sociais que se apresentam (ADDOR, 2016). Em razão disso, para fins de pesquisa deste trabalho, a perspectiva sobre democracia utilizada será a apresentada por Dahl (1998), na qual o sistema democrático deve estabelecer instituições e procedimentos que permitam ao Estado assegurar direitos fundamentais e a proteção das liberdades individuais aos seus cidadãos.

Com o intuito de fortalecer o sistema democrático, é possível verificar nas últimas décadas o desenvolvimento de diferentes instrumentos para a difusão de práticas de participação com o intento de inserir os cidadãos no processo de criação, monitoramento e intervenção nas políticas públicas (AVRITZER, 2009). Nesse viés, diversos autores apontam as tecnologias disruptivas como artefatos valiosos para inovações práticas no campo democrático (COLOMBO, 2006).

A difusão das Tecnologias da Informação e da Comunicação (TICs) nas últimas décadas tem criado um vasto leque de oportunidades para reconfigurar o sistema político. O rápido intercâmbio de informações, a interatividade proporcionada pelas redes sociais, o potencial das plataformas de participação cidadã e a disseminação do acesso à internet por meio de computadores e celulares são alguns dos fenômenos que alimentam a esperança de avançar em novas técnicas e métodos, buscando a consolidação de uma democracia efetiva (DE ALMEIDA, BAUTISTA & ADDOR, 2017).

Seguindo essa tendência, os governos ao redor do mundo têm adotado novas tecnologias como instrumentos para transformar a administração pública e trazer benefícios significativos em termos de eficiência, transparência, participação cidadã e tomada de decisões (FOUNTAIN, 2001; MOON, 2002; MAIER & SCHOLL, 2017). Assim, a adoção responsável das TICs pode levar a uma administração mais ágil, responsiva e orientada para o cidadão, no sentido de atender melhor às demandas sociais.

Contudo, a conjuntura vigente, marcada pela proliferação das TICs, imersão em redes digitais e preponderância de algoritmos, passa a estruturar uma reconfiguração das relações de poder na sociedade (DE ANDRADE et al, 2022). Hamelink (1997) enfatiza que a implementação de TICs pode fortalecer tendências históricas de desenvolvimento socioeconômico, resultando em um aumento das disparidades e desigualdades entre aqueles que possuem poder e conhecimento e aqueles que são excluídos.

Para mais, tais tecnologias oferecem ferramentas poderosas para o monitoramento e controle da população, permitindo um exercício de vigilância sem precedentes (DE ANDRADE et al, 2022). A proliferação de câmeras de vigilância, a coleta massiva de dados pessoais e a capacidade de monitorar as comunicações online são exemplos de práticas que levantam preocupações sobre direitos referentes à privacidade e à liberdade individual. Além disso, o uso de tecnologias para analisar dados e identificar comportamentos suspeitos pode resultar em perfis de vigilância, que potencialmente discriminam certos grupos sociais e ameaçam a igualdade de tratamento perante a lei (ELIAS, 2021; DE ANDRADE et al, 2022).

A personalização do consumo de informações proporcionada pelas TICs também apresenta desafios para a formação de uma opinião pública democrática (HAMELINK, 1997, MAGRANI, 2021). Essa personificação dos conteúdos da rede,

feita a partir das características de navegação de cada pessoa, cria um universo particular *on-line*, condicionando sua navegação. Nesse sentido, Magrani (2021), a *internet* estaria se transformando em um espaço no qual apenas conteúdos considerados de interesse do usuário lhe são apresentados, ocultando o que o usuário realmente deseja ou precisa ver. Nesse ínterim, o autor indica que a atual era tecnológica pode implicar restrições a direitos fundamentais como acesso à informação, liberdade de expressão, bem como à própria autonomia dos indivíduos. A falta de esferas de debates e a ilusão de consenso podem minar os princípios da democracia deliberativa e prejudicar a capacidade dos cidadãos de tomar decisões informadas (MAGRANI, 2021). Como indica Sérgio Amadeu da Silveira (2019, p. 51), se o poder na Sociedade da Informação gira em torno da comunicação, “a comunicação assimétrica pode anular as bases efetivas da democratização do poder”.

Tendo em vista o momento atual de declínio de regimes democráticos no mundo evidenciado nos relatórios *Autocratization Changing Nature?* do *V-Dem Institute*, e no *Democracy Index*, do *The Economist Intelligence*, torna-se imperiosa a investigação acerca dos potenciais riscos que o uso pela gestão pública das TICs, no caso deste trabalho a Inteligência Artificial, pode oferecer à democracia. À vista do grande potencial dessas tecnologias para estabelecer novos meios de participação política, maior disseminação de informações, trazer melhorias na oferta de serviços públicos e no atendimento às demandas sociais, cabe também evidenciar como as ferramentas de Inteligência Artificial podem fortalecer a democracia. Portanto, as próximas seções serão dedicadas a pontuar e aprofundar os principais benefícios e riscos para a democracia trazidos a partir da aplicação de tecnologias pela gestão pública.

### **2.1.1 Democracia, Tecnologias e Eficiência na Gestão Pública**

As últimas décadas foram marcadas pelo crescimento do papel do Estado brasileiro na garantia de serviços sociais, como educação, saúde, previdência, habitação e assistência social. Além disso, o Estado passou a intervir fortemente na regulação do sistema econômico de modo a regulamentar praticamente todas as atividades produtivas a fim de evitar os grandes problemas sociais causados pelas crises econômicas do século 20. Com o aumento das responsabilidades estatais na garantia dos direitos sociais e na regulação da atividade econômica, a eficiência

tornou-se um princípio essencial para a administração pública (BRESSER-PEREIRA, 1999, p. 11).

Eficiência é comumente compreendida na teoria econômica como o melhor uso dos recursos de uma organização, de modo a obter seu produto ou serviço (ARAGÃO, 1997). Nesta noção, poderia ser sintetizada na relação entre o *input* real e o *input* desejado pela organização, cujo resultado tenderia a zero. Ao adentrar no campo da administração pública, a eficiência, pautada nessa lógica econômica e sob os moldes da administração privada, inicialmente foi associada unicamente à ideia de corte de custos relativos a recursos humanos, materiais e financeiros com o intuito de fornecer o retorno máximo dos contribuintes.

Todavia, tal lógica perdeu forças logo no início de sua implementação, tendo em vista que a busca excessiva pela utilização ótima dos recursos impediu a flexibilidade e a capacidade inovativa da administração pública (ARAGÃO, 1997). Nesse sentido, por ser baseada apenas na ótica econômica racional, a estratégia de busca pela eficiência à época ignorava o aspecto político, que estava relacionado à necessidade de prestar serviços públicos para garantia de direitos fundamentais dos cidadãos. Essa ênfase na eficiência econômica ofuscou um aspecto importante para a gestão pública que é o da efetividade. Aragão (1997, p. 107) descreve a efetividade como a “relação, ao longo do tempo, entre os resultados alcançados e os objetivos pretendidos, sendo, muitas vezes, descrita como uma dimensão qualitativa do resultado (o valor social do produto).” (ARAGÃO, 1997). Na perspectiva da autora, na entrega de serviços públicos, não vale ser eficiente se não for efetivo.

Gabardo (2012) indica que a eficiência não pode se resumir ao aspecto econômico, critério que é atribuído à economicidade. Dessa forma, a noção de eficiência aplicada à gestão pública baseada apenas na utilização ótima e racional dos recursos com foco interno na gestão torna-se ultrapassada. A perspectiva trazida por Nohora (2018, p. 92) parece mais razoável, a qual afirma que “a eficiência impõe ao agente público um modo de atuar que produza resultados favoráveis à consecução dos fins que cabe ao Estado alcançar”. Com isso, o agente público deve desenvolver suas atividades de modo que, na gestão dos recursos públicos, seja observada a relação entre os meios utilizados e os resultados obtidos, mantendo como meta o interesse público e a garantia dos direitos sociais. (DESORDI & BONA, 2020).

Cabe destacar que o princípio da eficiência está presente no artigo 37 da Constituição Federal de 1988, que dispõe das normas elementares para nortear a

administração pública direta e indireta no Brasil, o qual apresenta tanto o sentido de otimização dos recursos quanto em promover o melhor desempenho possível das atribuições inerentes ao agente público com o objetivo de obter serviços com mais qualidade para os cidadãos (DI PIETRO, 2005; MORAIS, 2009).

Nesse íterim, pode-se relacionar o princípio da eficiência à visão da democracia para Dahl (1998), que pressupõe políticas públicas baseadas no atendimento ao interesse público, ou seja, na garantia dos direitos dos cidadãos. Desse modo, ao tratar a eficiência como a busca por métodos que atendam cada vez melhor as demandas sociais, instrumentos que tornem a administração pública mais eficiente também representam elementos fortalecedores da democracia.

A gestão pública enfrenta diariamente o desafio de atingir graus satisfatórios de eficiência por motivos como déficit de pessoal e de recursos financeiros (DESORDI & BONA, 2020), além de razões como má gestão, a existência de obstáculos burocráticos e as dificuldades em controlar eventuais fraudes e atitudes corruptas no âmbito dos órgãos públicos (ARAÚJO, ZULLO & TORRES, 2020). Tais fatores geram insatisfação interna e externa pela carência na prestação do serviço público e o gestor público carece, assim, de artefatos alternativos para alcançar a eficiência administrativa almejada e garantir benefícios democráticos (DESORDI & BONA, 2020).

Fountain (2001) e Desordi & Bona (2020) destacam as inovações tecnológicas como mecanismos com alto potencial para aumentar a eficiência da administração pública, ao possibilitar a automatização de processos administrativos. A implementação responsiva de sistemas de informação integrados e o uso de soluções tecnológicas avançadas podem simplificar tarefas administrativas, reduzindo o tempo e os recursos necessários para executá-las, além de promover aumento da produtividade (DIAS, SANO & MEDEIROS, 2019). Nesse sentido, o uso adequado dessas novas tecnologias pode possibilitar o aumento da eficiência na administração pública, resultando em uma administração mais ágil e na melhoria dos serviços prestados aos cidadãos.

Em suma, adota-se como recorte de análise para este trabalho a noção de que a utilização adequada e responsável de tecnologias disruptivas para aumento da eficiência na gestão pública se configura como um elemento fortalecedor da democracia, uma vez que pode permitir o aperfeiçoamento das atividades públicas e permitir a entrega de serviços cada vez melhores para os cidadãos. Cabe, agora,

discutir como o uso de tecnologias pela gestão pública pode fornecer subsídios para fortalecer o papel dos cidadãos em um contexto de democracia participativa.

### **2.1.2 Democracia Participativa e Tecnologias aplicadas à Gestão Pública**

O uso de tecnologias pela gestão pública podem ser uma solução para aprimorar a relação entre Estado e cidadãos, de modo a evitar que o Estado se torne um ente distante da população e indiferente às suas demandas (SANTANA, 2008). Sabe-se que existem diferentes instâncias de participação cidadã, todavia, tal ponto não é central nesta discussão. Para este trabalho, compreende-se que democracia exige participação no agir público, e a gestão pública precisa fornecer insumos para garantir que os cidadãos possam monitorar as ações governamentais, bem como para facilitar a inclusão dos cidadãos no processo de formulação e execução de políticas públicas (JALOTO & MOREIRA, 2023).

Cabe ressaltar que a participação cidadã em um contexto democrático também se dá por meio dos direitos, garantias e demais instrumentos judiciais e extrajudiciais (JALOTO & MOREIRA, 2023). Desse modo, instrumentos utilizados pela administração que proporcionem a garantia de direitos fundamentais são benéficos à democracia. De maneira oposta, instrumentos que violem direitos fundamentais ou que não proporcionem a democratização dos serviços públicos, são considerados evidentes riscos à democracia.

A partir da noção de que instrumentos adotados pelos governos que permitam o envolvimento dos cidadãos nas tomadas de decisões e no monitoramento das ações governamentais são valiosos para a democracia participativa, é possível destacar o uso de inovações tecnológicas como ferramentas para a consolidação da democracia (DE ALMEIDA, BAUTISTA & ADDOR, 2017). Estes autores indicam que é possível distribuir as potencialidades trazidas pelas tecnologias disruptivas para a democracia em 4 pilares: I. acesso amplo e democrático à informação; II. ampliação da participação à distância; III. desburocratização dos processos; e IV. capacidade de mobilização.

A primeira potencialidade diz respeito à facilidade de troca de informações promovida pelo caráter dinâmico dos sistemas *online*. Tal elemento pode ser um instrumento importante para a democracia, uma vez que permite a ampla disponibilidade de informações ao público para qualificar a participação dos cidadãos

nos debates e decisões públicas. É importante ressaltar que, o poder público, por sua vez, deve manter a transparência em seus propósitos e ações, uma vez que apenas com clareza de objetivos é possível que a tomada de decisões seja um processo satisfatório (PINTAUDI, 2004). Assim, os mecanismos tecnológicos de acesso à informação permitem que os cidadãos deixem “de ser meros sujeitos passivos, consumidores de políticas e assumem postura ativa, deliberando sobre as escolhas de seus representantes” (BERNARDES e MEZZARROBA, 2010, p.7).

Ademais, as ferramentas tecnológicas, ao criarem um campo de oportunidades para retomada da participação nas decisões governamentais, impulsionam o controle social. Este, por sua vez, se refere a efetiva participação do cidadão na gestão da máquina pública, em especial na luta contra a corrupção (ARAÚJO, ZULLO & TORRES, 2020), elemento que, conforme Castells (2018), contribui para o agravamento da atual crise nas democracias liberais. Assim, o controle social aliado ao controle institucional, exercido pelos órgãos fiscalizadores, favorece a correta aplicação dos recursos públicos, visando ao efetivo atendimento às demandas da sociedade e fortalecimento da democracia (KRUG & LEAL, 2021).

Contudo, estudos de Santana (2008) revelam que as potencialidades de novas tecnologias não são exploradas totalmente pela gestão pública brasileira. O autor aponta que as novas tecnologias vêm sendo utilizadas em sua maioria apenas para disponibilizar os dados para promover explicitação das decisões e responsabilização dos atores. No entanto, o autor ressalta que apenas deixar os dados e informações disponíveis aos usuários/cidadãos, apesar de fundamental, não é suficiente para garantir que tais informações sejam de fácil interpretação por parte da população. Nas palavras de Nohora e Colombo (2019, p. 94), “informação disponível não é, necessariamente, informação acessível.”.

Nesse panorama, o uso de tecnologias que atuem de modo a facilitar a interpretação e utilização de dados podem trazer benefícios para a transparência pública e, portanto, para o exercício democrático. Ademais, é preciso ressaltar que em um país como Brasil, marcado pelo alto grau de desigualdade socioeconômica, permitir que o meio principal de acesso a informações seja por meio do uso de *internet*, pode gerar riscos à democracia por deixar cidadãos sem capacidade de acesso a tais tecnologias alheios a esses dados.

Ademais, tecnologias disruptivas que permitam condensar e promover análise sistemática de dados acerca das demandas cidadãs, trazendo *insights* significativos

para gestores públicos ao permitir uma avaliação mais precisa dos problemas e desafios encontrados (MAIER & SCHOLL, 2017), também são tendências governamentais no mundo afora e trazem benefícios democráticos. Tais tecnologias são elementos valiosos para a tomada de decisão, uma vez que permitem o agrupamento de um número expressivo de informações cujo esgotamento de análise iria além da capacidade humana. Contudo, caso as tecnologias sejam utilizadas de modo a priorizar demandas para favorecer determinados grupos sociais, podem, de maneira oposta, oferecer riscos democráticos.

Já a segunda perspectiva trazida por Almeida, Bautista & Addor (2017), diz respeito ao uso de tecnologias para facilitar espaços públicos de debate e tomada de decisões, superando a barreira das distâncias físicas e do tempo. Segundo os autores, as inovações tecnológicas permitem uma mudança nas limitações geográficas e financeiras que, em geral, são colocadas como restritivas para o estabelecimento de espaços participativos amplos.

A terceira potencialidade desenvolvida pelos autores relaciona-se ao uso de tecnologias para redução da burocracia entre cidadãos e seus representantes (ALMEIDA, BAUTISTA & ADDOR, 2017). O uso de *softwares*, aplicativos e *chatbots* permite maior integração entre os cidadãos e seus representantes. Assim, o emprego de tecnologias inovadoras pela gestão pública que permitam uma troca mais dinâmica e fácil entre Estado e cidadão torna-se um meio de aperfeiçoamento da capacidade de acompanhamento por parte da população das ações realizadas pelo governo (GUIMARÃES e MEDEIROS, 2005; ALMEIDA, BAUTISTA & ADDOR, 2017). Todavia, é preciso considerar a conjuntura de grande desigualdade social e econômica e de acesso precário aos mais diversos direitos que o brasileiro enfrenta. Por isso, não se pode pressupor que todo cidadão terá acesso ao celular, ao computador e à internet, ou mesmo que tenha competência técnica para utilizá-la de forma satisfatória (DA SILVA, OTTONICAR, YAFUSHI, 2017). Assim, o caráter excludente das tecnologias ainda se configuram como um obstáculo para que tais instrumentos cumpram um papel democrático.

A quarta e última potencialidade abordada por Almeida, Bautista & Addor (2017) diz respeito a como o uso das Tecnologias de Informação e Comunicação (TICs) transformou a capacidade de organização e mobilização política da sociedade civil. Apesar de não ser um elemento de interação direta entre Estado e sociedade civil, a internet e as redes sociais têm apresentado grande impacto no exercício

democrático da população. Com o uso dessas ferramentas, os cidadãos passaram não apenas a trocar informações relevantes sobre as questões públicas, mas a também ter maior capacidade de construção de movimentos políticos mais horizontais, democráticos e participativos.

A partir do exposto, percebe-se que o uso de tecnologias inovadoras tem atuado de modo a transformar a relação entre Estado e sociedade, oferecendo benefícios e riscos para a participação cidadã. Não obstante, os instrumentos governamentais baseados nessas tecnologias podem remodelar a gestão pública, ao permitir o aumento de eficiência dos processos administrativos e/ou operacionais e, dessa forma, melhorias nos serviços prestados aos cidadãos, aperfeiçoando o pacto democrático. Cabe, agora, apresentar o que são inovações tecnológicas e trazer as concepções necessárias acerca da ferramenta que será objeto de estudo deste trabalho: a Inteligência Artificial (IA).

## **2.2 Inovações Tecnológicas na Gestão Pública**

Devido ao crescimento do papel do Estado na vida dos cidadãos nos últimos anos, os governos em todo o mundo têm enfrentado constantes pressões da sociedade para responder às necessidades dos cidadãos e fornecer serviços públicos mais responsivos, transparentes, sustentáveis e democráticos (KLUMB & HOFFMANN, 2016). Nesse sentido, é possível destacar como os principais desafios enfrentados pelo governo no século XXI a globalização, o combate à desigualdade, a retomada da confiança nos governos, o respeito à diversidade, a busca pela boa governança e por uma gestão pública mais eficiente (SCHWELLA, 2005; BRANDÃO & BRUNO-FARIA, 2013). De modo a responder tal questão, a criatividade e adoção de instrumentos inovadores são essenciais para que a administração pública ofereça um novo padrão de serviços capaz de considerar a complexidade de problemas no atendimento às demandas sociais.

Os estudos de Potts e Kastle (2010) revelam que, sob o ponto de vista social, um setor público inovador que disponibiliza produtos e serviços de boa qualidade, considerando sua facilidade de uso, acessibilidade e oportunidade, pode estabelecer uma relação mais eficaz com os cidadãos. Ademais, a eficiência do setor público de um país e a entrega de serviços públicos de boa qualidade são de extrema importância

para atingir operações mais transparentes, o que pode gerar maior satisfação por parte dos beneficiários em relação aos serviços oferecidos e promover um aumento no nível de confiança no setor público (VIGODA-GADOT et al, 2008; BRANDÃO & BRUNO-FARIA, 2013). É nesta conjuntura que a adoção de inovações tecnológicas pela administração pública vem se tornando um tema estratégico, essencial para aperfeiçoamento da gestão estatal e da democracia.

Os primeiros trabalhos sobre inovação tratavam acerca da relação entre inovação tecnológica e desenvolvimento econômico e tinham enfoque no desenvolvimento de produtos e processos com aplicação comercial no setor privado. Schumpeter (1982) foi o precursor da corrente teórica que alça a inovação como elemento-chave da dinâmica econômica, ao explicar a inovação como a mudança técnica e/ou tecnológica bem-sucedida capaz de fornecer vantagem competitiva para os países ou regiões. Em sua teoria, identificou cinco tipos de inovação: novos produtos ou mudanças substanciais em produtos existentes (inovação tecnológica de produto); novos processos ou métodos de produção (inovação tecnológica de processo); novos mercados; novas fontes de recursos e novas organizações. Nesta perspectiva, a inovação vai além de questões tecnológicas, incluindo também o atendimento das necessidades dos clientes (STAL, 2007).

Com a ampliação de estudos acerca da inovação em outros setores, novas definições foram ampliando seu escopo, descrevendo também inovações no setor público. Van de Ven et al (2000) definem inovação como o processo de desenvolver e implementar novas ideias. Mulgan e Albury (2003) apresentam a inovação no setor público como a criação e a implementação de novos produtos, processos, métodos e técnicas de oferta de serviços públicos, que pressupõem melhor desempenho em termos de eficiência, eficácia e efetividade de resultados do setor público para a sociedade. Assim, inovação no setor público pode ser compreendida neste trabalho como uma ideia - nova, melhorada ou reformulada - e sistematizada para o contexto de sua aplicação, com o intuito de solucionar um problema de interesse público.

O século XXI vem sendo marcado pelo advento da Quarta Revolução Industrial, ou indústria 4.0, a qual tem como fundamento a revolução digital. Klaus Schwab (2016), primeiro ao adotar o termo Quarta Revolução Industrial, indica que esse período é marcado por "uma Internet muito mais ubíqua e móvel, por sensores menores e mais poderosos que se tornaram mais baratos e pela inteligência artificial e aprendizado de automática (ou aprendizado de máquina)." (SCHWAB, K., p.16,

2016). Diversos são os tipos de inovações tecnológicas que se destacam na indústria 4.0: biotecnologia, computação em nuvem, impressão 3D, robótica, IoT (internet of things), *Big Data*, *blockchain*, realidade virtual e aumentada, inteligência artificial e outras (SAVÉRIO & NICOLAS, 2022; GOMES & MARTINHO, 2023).

Nesse sentido, não apenas o setor privado, mas o setor público vem sendo impactado de forma profunda pelas inovações tecnológicas provenientes da Quarta Revolução Industrial. Dentre essas tecnologias que vêm transformando a gestão pública, uma se apresenta como bastante promissora: a Inteligência Artificial, objeto de análise deste trabalho. Apesar de ser um fenômeno que teve origem no século XX, sua aplicação no setor público é recente, e requer análises e reflexões para que seja aperfeiçoada. Cabe, agora, apresentar alguns de seus conceitos básicos e explicitar como vem ocorrendo sua aplicação na gestão pública, apontando possíveis benefícios e riscos que seu uso pode apresentar ao sistema democrático.

### 2.2.1 Inteligência Artificial

Antes de compreender do que se trata Inteligência Artificial, é necessária certa noção acerca de algoritmos. Elias (2021) define algoritmos como

*[...] uma sequência de regras ou operações que, aplicada a um número de dados, permite solucionar classes semelhantes de problemas. Na informática e telemática, o conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número de etapas. Em outras palavras mais claras: são as diretrizes seguidas por uma máquina. Na essência, os algoritmos são apenas uma forma de representar matematicamente um processo estruturado para a realização de uma tarefa (ELIAS, 2021, p. 1, grifo do autor).*

Desse modo, algoritmos podem ser entendidos como conjuntos de instruções passo a passo que resolvem um problema ou realizam uma tarefa específica, sendo a base sobre a qual muitos sistemas de IA são construídos (ELIAS, 2021). Nesse sentido, os algoritmos desempenham um papel fundamental na IA.

Em razão da sua complexidade, não é possível resumir Inteligência Artificial a uma única definição. Gabriel (2018, p. 185) define IA como “a área da Ciência da Computação que lida com o desenvolvimento de máquinas/computadores com capacidade de imitar a inteligência humana”. Peixoto e Silva (2019), apresentam IA como a repetição artificial da capacidade de adquirir e aplicar habilidades e conhecimentos diversos para resolver um dado problema, solucionando-o,

raciocinando e aprendendo com as situações. Assim, a IA consiste no desenvolvimento de sistemas computacionais capazes de realizar tarefas que normalmente requerem habilidades intelectuais humanas (DESORDI & BONA, 2020).

Para a OCDE (2019), a inteligência artificial pode ser compreendida como um sistema inteligente capaz de fazer recomendações e previsões com os dados que o alimentam e operar com certos níveis de autonomia. Para operar dessa forma, é preciso que humanos forneçam esses dados e o façam com objetivos pré-definidos. O ciclo de vida da IA, por sua vez, envolve algumas fases, que podem ou não ocorrer numa certa ordem, sendo elas: 1) definição dos dados e modelos de processamento; 2) verificação e validação dos modelos; 3) implementação; e 4) operação e monitoramento (OCDE, 2019).

O aprendizado autônomo se dá através do *machine learning* (aprendizado de máquina), subcampo da IA, o qual

É um ramo da inteligência artificial que envolve a criação de algoritmos que podem aprender automaticamente a partir de dados. Ao invés de os desenvolvedores de *software* elaborarem enormes códigos e rotinas com instruções específicas para que a máquina possa realizar determinadas tarefas e conseguir resultados (e com isso limitar drasticamente o seu campo de atuação e resultados), no aprendizado de máquina *treina-se o algoritmo para que ele possa aprender por conta própria*, e até mesmo conseguir resultados que os desenvolvedores dos algoritmos nem mesmo poderiam imaginar. Neste treinamento, há o envolvimento de grandes quantidades de dados que precisam ser alimentadas para o algoritmo (*ou aos algoritmos envolvidos*), permitindo que ele (o algoritmo) se ajuste e melhore cada vez mais os seus resultados. (ELIAS, 2021, p. 2, grifo do autor).

Assim, *machine learning* pode ser entendida como uma abordagem computacional capaz de detectar padrões de modo automático, sem serem explicitamente programados, e utilizar tais padrões para previsão de dados futuros ou para aprendizagem e tomada de decisões.

Já a *deep learning*, ou aprendizagem profunda, dispõe da aptidão de transformar vastos volumes de dados em informação útil (ELIAS, 2021). O *deep learning* é uma abordagem que utiliza redes neurais artificiais com múltiplas camadas (também conhecidas como redes neurais profundas). Essas redes neurais profundas são inspiradas na estrutura e funções do cérebro humano, na interligação de neurônios, dando origem às redes neurais artificiais. Por intermédio do *deep learning*, tarefas que são tradicionalmente desempenhadas pelos seres humanos, como tomada de decisões, classificação de imagens, tradução automática, reconhecimento facial, reconhecimento de voz e tradução. Além de outras funções que superam a

capacidade de raciocínio humano, como o manejo e processamento de grandes bases de dados, estão sendo executadas por máquinas inteligentes, permitindo que o ser humano ganhe tempo e se ocupe de tarefas mais complexas e subjetivas que exigem a inteligência humana para execução (ELIAS, 2021).

A IA e a *Internet* das coisas estão intrinsecamente relacionadas. Elias (2021) explica essa inter-relação comparando-a ao vínculo entre cérebro e o corpo humano. Assim,

Nossos corpos coletam as entradas sensoriais, como visão, som e toque. Nossos cérebros recebem esses dados e dão sentido a eles, por exemplo, transformando a luz em objetos reconhecíveis, transformando os sons em discursos compreensíveis e assim por diante. Nossos cérebros então tomam decisões, enviando sinais de volta para o corpo para comandar movimentos como pegar um objeto ou falar. Todos os sensores conectados que compõem a Internet das coisas (Internet of things) são como nossos corpos, eles fornecem os dados brutos do que está acontecendo no mundo. A inteligência artificial é como nosso cérebro, dando sentido a esses dados e decidindo quais ações executar. E os dispositivos conectados da Internet das coisas são novamente como nossos corpos, realizando ações físicas ou se comunicando com os outros. (ELIAS, 2021, p. 3).

Para mais, é importante mencionar que, a difusão crescente do uso da *Internet* pela sociedade em geral criou um ambiente no qual a geração de dados progride de modo extremamente acelerado. O armazenamento e o tratamento da volumosa quantidade de dados podem ser alocados no que se conhece por *Big Data*, sendo que sua disponibilização para toda a sociedade se dá pelo *Open data* (GOMES & BRAGA, 2017; SOARES, 2018). Nota-se, portanto, que a IA se escora no volume de dados disponível processados pelo *Big Data* para formação de seus sistemas.

O *machine learning* e o *deep learning* são novidades da Indústria 4.0 que trouxeram grandes avanços para a Inteligência Artificial nos últimos anos. Tanto o *machine learning* quanto o *deep learning* requerem uma quantidade volumosa de dados para operar de forma eficaz, e tais dados estão sendo constantemente coletados por bilhões de sensores que se conectam à *Internet* das Coisas diariamente.

Apesar do grande potencial da IA e de seus subcampos para auxiliar o ser humano na execução de atividades cotidianas, é de extrema importância destacar que, por trás de qualquer solução de inteligência artificial existem seres humanos que pensaram no seu propósito, elaboraram um algoritmo e definiram em quais dados esse algoritmo iria se apoiar (SCHULER & MONTARDO, 2020). Tal fator transfere para o sistema inteligente aspectos de parcialidade transmitidos de forma consciente

ou não e que influenciam diretamente na saída de dados que será gerada pela tecnologia, não importando que esta seja capaz de aprender de forma autônoma. Elias (2021) notabiliza que a transmissão de vieses humanos para os algoritmos é denominada como “*Machine bias*”, “*Algorithm bias*” ou simplesmente, *Bias*.

À vista do exposto, percebe-se que instrumentos baseados em IA são inovações tecnológicas que podem apoiar a gestão pública a utilizar com maior eficiência os dados sob sua tutela na resolução de problemas, bem como pode trazer riscos à sociedade no manejo inadequado desses dados. Nesse sentido, passa-se a discutir o uso de ferramentas de IA na gestão pública.

### **2.2.2 IA na Gestão Pública**

Governos ao redor do mundo têm se interessado em explorar o uso da Inteligência Artificial para aprimorar seus serviços públicos e atender melhor às crescentes demandas sociais. Segundo Van Noordt e Misuraca (2022), a adoção de tecnologias de IA pela gestão pública pode fornecer grandes benefícios e valor público para os cidadãos, a depender da forma como são empregados.

O uso de IA no setor público apresenta grande potencial para automatizar processos, ao tornar atividades repetitivas mais simples, dispensando a atuação humana em casos concretos, a favor de aumentar a velocidade dos procedimentos (DESORDI & BONA, 2020; DA SILVEIRA, 2017), ou para ampliar a capacidade de processamento de dados por parte dos tomadores de decisão humanos (CAMPOS & FIGUEIREDO, 2021). Assim, pode ser tratada como uma ferramenta capaz de aperfeiçoar o ciclo de políticas públicas (CAMPOS & FIGUEIREDO, 2021; VAN NOORDT & MISURACA, 2022). De acordo com Araújo, Zullo e Torres (2020),

A partir de uma grande base de dados, os algoritmos podem, por exemplo, identificar padrões de comportamento do contribuinte, reconhecer grupos populacionais que necessitam de cuidados específicos de saúde por apresentarem maior risco médico e contribuir para uma gestão pública mais eficiente em diversas outras situações. Isso permite que os governos atuem de forma preditiva, ao invés de agir apenas em reação a determinada necessidade da população. (ARAÚJO, ZULLO & TORRES, 2020, p. 248).

Desse modo, os instrumentos de IA vêm sendo considerados como ferramentas bastante pertinentes ao processo de formulação de políticas públicas. Desouza e Jacob (2017) indicam que tais tecnologias podem auxiliar nessa etapa do

ciclo de políticas públicas ao contribuir para que a política pública se baseie cada vez mais em dados concretos, além de permitir que a etapa de tomada de decisões seja baseada em análises melhores, mais precisas e menos incertas.

O uso de tecnologias de IA pode facilitar a identificação dos problemas públicos e as demandas dos cidadãos com mais precisão, rapidez e eficiência do que técnicas tradicionais como *surveys* (PENCHEVA, ESTEVE & MIKHAYLOV, 2020). Ao detectar problemas públicos com mais precisão e rapidez, a tecnologia auxilia na obtenção de soluções mais rápidas antes que eles se agravem. A IA também pode auxiliar no processo de tomada de decisão ao criar alternativas de políticas e possibilitar a análise dos interesses dos cidadãos em relação a diversas opções de políticas ou melhorar a participação dos cidadãos na elaboração de políticas alternativas, fortalecendo a democracia (DESOUZA & JACOB, 2017).

Não obstante, Van Noordt e Misuraca (2022) salientam que uso da IA no processo de formulação de políticas públicas também tem sido como uma forma de tornar o processo mais inclusivo, pois possibilita novas maneiras de incluir a participação dos cidadãos e dar voz àqueles que podem ser negligenciados pelos métodos tradicionais. A análise de dados provenientes das redes sociais pode sistematizar e deixar mais claras as preferências dos cidadãos para o desenho de novas propostas de políticas públicas, permitindo a consideração das discussões nas redes sociais dentro do debate público (CARDULLO & KITCHIN, 2019; VAN NOORDT & MISURACA, 2022).

O uso da IA também vem sendo empregado para melhorar a entrega de serviços públicos. Os estudos de Pencheva, Esteve & Mikhaylov (2020), indicam que a combinação de *Big Data* e IA tem potencial de melhorar significativamente o desempenho do governo e a eficiência na prestação de serviços públicos, economizando recursos e aumentando a produtividade. Ao agrupar fontes de dados variadas e agrupar os usuários em grupos específicos, os serviços públicos podem ser adaptados para melhor atender às necessidades considerando as individualidades dos cidadãos, potencialmente aumentando a eficácia e a satisfação com serviços (VEALE & BRASS, 2019).

O atendimento ao cidadão também vem sendo impactado pela adoção da IA. *Chatbots* e assistentes virtuais baseados em IA podem fornecer suporte e atendimento ao cidadão ao responder perguntas frequentes, o que libera mais tempo para que os funcionários públicos realizem outras tarefas mais complexas (MEHR,

ASH & FELLOW, 2017). Contudo, caso essas ferramentas sejam o principal canal de comunicação, pode gerar prejuízos democráticos, devido ao grande cenário de exclusão digital no Brasil (DE ALMEIDA, BAUTISTA & ADDOR, 2017, BRASIL, 2020).

Um dos benefícios mais comumente mencionados do uso de IA na gestão pública liga-se a sua capacidade de detecção automatizada de fraudes e auxiliar no combate à corrupção (SAVÉRIO & NICOLAS, 2020). Segundo os autores, a IA pode ser utilizada para identificar transações fraudulentas, seja fraudes cometidas por cidadãos ou para combater a corrupção por parte dos agentes públicos, além de aumentar as possibilidades de realização de auditorias por órgãos de controle externo. Tal fator é bastante positivo, tendo em vista que a corrupção tende a reduzir a eficiência da gestão pública, ao reduzir as suas capacidades estatais (TOYOSHIMA & LOPES, 2013). Um exemplo de utilização dessas ferramentas de combate à fraude e à corrupção no Brasil refere-se ao caso do Tribunal de Contas da União (TCU), o qual encontrou na utilização de ferramentas de inteligência artificial uma forma de promover aumento da eficiência de sua produção (DESORDI & BONA, 2020; SAVÉRIO & NICOLAS, 2022).

Apesar de suas potencialidades, o uso da IA no setor público enfrenta riscos a serem considerados. Um dos principais riscos do uso de IA para a democracia refere-se a sua falta de transparência. Segundo Fornasier (2021):

A coleta massiva de dados visa a obtenção de garantia devido a dois tipos de opacidade que surgem como resultado da tal coleta: opacidade técnica (dificuldade para os cidadãos entenderem a tecnologia por trás da coleta de dados em massa), e opacidade algorítmica (resultante de propriedades inerentes a algoritmos que orientam a coleta e o processamento de dados em massa). (FORNASIER, 2021, p. 197).

Araújo, Zullo e Torres (2020) salientam que a ausência de transparência se choca com os princípios que norteiam a Administração Pública. O primeiro trata-se da violação clara do princípio da publicidade, o que impede o controle social, exercido pelos cidadãos, e o controle institucional de órgãos fiscalizadores, o que configura. Nesse viés, a falta de transparência algorítmica também pode comprometer a legitimidade democrática da decisão estatal. A transparência é um dos pilares da democracia liberal, uma vez que permite ao cidadão informações quanto às razões de agir da gestão pública, sendo que a ausência de divulgação fere direitos fundamentais e torna inválida a decisão tomada.

Além da falta de transparência, Araújo, Zullo e Torres (2020) e Fornasier (2021) apontam que o processo decisório da IA pode refletir algum viés discriminatório se o sistema aprender a partir de dados discriminatórios. Os dados processados pelos computadores são extraídos das ideias e concepções encontradas na sociedade. Logo, se a base de dados tratada pelo algoritmo for extraída de um ambiente que propaga preconceitos e comportamentos discriminatórios, o resultado do tratamento dessa base de dados poderá reproduzir esses comportamentos, representando riscos democráticos. Em outras palavras, se os dados de treinamento forem tendenciosos, o sistema de IA corre o risco de reproduzir esse viés (FORNASIER, 2021).

Esse problema, quando repetido institucionalmente pelo poder público, torna-se uma questão extremamente crítica e alarmante. O controle social e democrático acerca das características dos dados utilizados é essencial para que os vieses discriminatórios não sejam reproduzidos pelas máquinas (FORNASIER, 2021). A simples ideia de que atos formalmente realizados por uma autoridade pública para propagar comportamentos discriminatórios, é um fator que pode representar enormes riscos à confiança no Estado e, assim, no modelo democrático, contribuindo para a atual crise nas democracias liberais abordada por Castells (2018).

Alguns exemplos de aplicações de IA que poderiam acarretar discriminação apontados por Fornasier (2021) são: i. recrutamento e seleção; ii. prevenção e repressão de crimes; e iii. reconhecimento facial. O primeiro exemplo diz respeito à possibilidade dos algoritmos de IA serem treinados em dados históricos que refletem preconceitos e desigualdades existentes, como gênero ou raça, os quais podem ser perpetuados durante o processo de seleção de candidatos. O segundo exemplo, por sua vez, associa-se ao uso de algoritmos de IA usados em sistemas de justiça criminal, como na definição de sentenças ou na determinação de liberdade condicional, podem apresentar viés racial ou socioeconômico se forem alimentados com dados que refletem desigualdades históricas. O último exemplo diz respeito à sistemas de reconhecimento facial baseados em IA que apresentem dificuldades em reconhecer corretamente pessoas com tons de pele mais escuros ou características faciais distintas, levando a erros de identificação e discriminação racial.

Segundo o relatório *Recomendações de Governança: uso de inteligência artificial pelo poder público*, as ferramentas de apoio à tomada de decisão adotadas internamente pelos órgãos governamentais despertam especial preocupação na sociedade civil. Estas ferramentas desempenham um papel crítico ao auxiliar os

agentes públicos na definição de ações que influenciam a vida das pessoas, impactando, de maneira direta ou indireta, o exercício de direitos fundamentais, podendo oferecer riscos democráticos (ELIAS, 2021). O principal risco concentra-se nos conjuntos de dados de treinamento e nos critérios empregados pelos modelos automatizados de previsão e classificação utilizados pelos órgãos governamentais. Existe o receio de que tais elementos possam reproduzir padrões discriminatórios já existentes na sociedade, afetando, especialmente, parcela mais socialmente vulnerável da população. Por tais razões, a supervisão e revisão de decisões automatizadas por parte dos agentes públicos é imperiosa, e seu descumprimento corre risco de violação do Art. 20 da LGPD.

Elias (2021) recomenda extremo cuidado por parte da administração pública contra qualquer tomada de decisão algorítmica que envolva a coleta de dados não consentida, ou não compreendida, bem como compartilhamento ou análise de dados pessoais dos cidadãos. Nas palavras do autor,

A importância dos direitos constitucionais de intimidade, da privacidade e autodeterminação informativa como um direito individual e uma característica de uma sociedade democrática deve ser cuidadosamente mantida ao longo dos desenvolvimentos tecnológicos. (ELIAS, 2021, P. 15).

Segundo Brasil (2020), existem meios práticos para eliminar ou mitigar os vieses dos algoritmos e dos dados que alimentam as tecnologias de IA (BRASIL, 2020). Um deles diz respeito à necessidade de verificação acerca da representatividade da equipe do projeto quando o objetivo é impedir que a máquina reproduza preconceitos existentes. Outro refere-se à disponibilidade dos dados escolhidos para o conjunto de treinamento do modelo para auditoria externa.

Para mais, Brasil (2020) destaca a importância de mecanismos de *accountability* e transparência para possibilitar que a sociedade civil exerça controle social sobre a utilização de ferramentas de inteligência artificial pelo poder público, visando a minimização dos riscos de violações a direitos. Segundo os autores, transparência e *accountability*, quando aplicadas a algoritmos públicos, significa fornecer acesso a informações públicas relativas aos algoritmos usados pelo setor público. Os autores apontam como alternativas para garantir a transparência a existência de algoritmos com códigos abertos e de mecanismos de transparência ativa, nos quais o cidadão possa solicitar via e-SIC (Sistema Eletrônico do Serviço de

Informações ao Cidadão) a relação de quais sistemas algorítmicos o setor público está usando, onde e como (BRASIL, 2020).

Ainda, quando há restrição de acesso por motivos de sigilo, como em casos de Segredo de Justiça Criminal, Brasil (2020) faz duas recomendações de mecanismos de transparência e *accountability* para permitir o controle social. De forma básica, o poder público deve fornecer, no mínimo, informações sobre as variáveis de entrada e saída do modelo, bem como o tipo de algoritmo utilizado pela ferramenta. Isso auxilia que as etapas do processo de aprendizado de máquina que levaram à ação da IA sejam rastreáveis e que as variáveis que influenciaram na tomada de decisão sejam tornadas públicas. A segunda sugestão refere-se à realização regular de auditorias no desempenho do algoritmo, realizadas por especialistas externos ao órgão público implementador. Isso visa verificar a eficácia do algoritmo em relação ao seu propósito e avaliar se a tecnologia pode promover algum impacto adverso a direitos fundamentais (BRASIL, 2020).

A partir do exposto, percebe-se que há visões otimistas acerca das potencialidades das ferramentas de IA para a gestão pública, tendo em vista sua capacidade de aumentar eficiência no processo administrativo e de abrir um novo leque para inclusão dos cidadãos nos processos comunicativos. Há, contudo, a possibilidade de riscos que demonstram que as tecnologias de IA devem ser desenvolvidas de modo democrático, com revisão das decisões automatizadas, com devida transparência acerca de sua aplicação e com interdisciplinaridade na sua construção de algoritmos. Por isso, apesar do alto potencial da IA para gerar benefícios para a sociedade, seus riscos não devem ser subestimados ou negligenciados.

### **2.2.3 Uso de recursos de IA na Segurança Pública**

Os Sistemas de Inteligência Artificial vêm apresentando aplicações potenciais na área de segurança pública. Com a evolução da capacidade computacional para coleta, entrecruzamento e tratamento de enormes volumes de dados disponíveis, a IA vem proporcionando a corpos policiais e de segurança a capacidade de processamento de um enorme volume de informações pessoais sobre os cidadãos. Com base nestas informações coletadas, é possível traçar perfis, classificar pessoas em função de prognósticos de risco, cruzar dados sobre investigações em curso,

reduzir o círculo de suspeitos, entre outras ações (DE MENEZES & SANLLEHÍ, 2021).

Dentre as principais aplicações da IA no campo da segurança pública, é possível citar: algoritmos de processamento de linguagem natural para identificação de ameaças à segurança pública, como discursos de ódio e incitação à violência, além de detecção de fraudes (BRASIL, 2021b); sistemas de análise de imagens e áudios; sistemas de reconhecimento facial para auxiliar na identificação de suspeitos e sistemas de classificação de imagens (BRASIL, 2020); técnicas de policiamento preditivo (DE LAAT, 2019; BRASIL, 2021b); e plataformas de cidades inteligentes e cidades seguras (DE SOUSA et al, 2023).

A utilização de algoritmos de processamento de linguagem natural na identificação de ameaças à segurança pública pode trazer várias melhorias aos serviços públicos nessa área. Dentre os benefícios potenciais, há a capacidade de realizar um monitoramento abrangente de conversas e atividades que possam representar perigos à segurança pública a partir da análise de dados de várias fontes, incluindo redes sociais, fóruns online e notícias (PRADHAN et al, 2019). Isso permite às autoridades acompanhar de perto discussões e planejamento de atividades suspeitas, mesmo em espaços virtuais, ampliando sua capacidade de prevenção e investigação de crimes.

Contudo, ferramentas de IA focadas em processamento de linguagem natural para estimar algum risco relacionado à segurança pública podem impactar negativamente pessoas de grupos sociodemográficos marginalizados (BRASIL, 2020). Nesta perspectiva, o algoritmo pode apresentar vieses contra pessoas de baixa renda que não dispõem de um bom domínio da norma culta da língua portuguesa ou que usam termos informais/abreviações/gírias. Tal risco não se restringe à segurança pública, e vieses contra grupos socialmente marginalizados podem ocorrer com o uso de IA de maneira geral, tendo suas consequências negativas potencializadas no caso da segurança pública, posto que muitas vezes resulta em privação de liberdade ou mesmo ameaça à vida (BRASIL, 2020).

Outra aplicação da IA na segurança pública diz respeito às soluções tecnológicas que permitem a identificação de objetos e de pessoas em imagens e vídeos. Essas aplicações abrangem desde detecção simples, como identificar uma pessoa pulando um muro, até capacidades mais complexas, como identificar pessoas portando armas ou agredindo outras pessoas nas ruas (BRASIL, 2021b; JUNIOR &

DOS SANTOS, 2022). A análise de áudio também tem ganhado destaque, com soluções capazes de detectar sons de tiros, batidas de carros ou tumultos, e enviar alertas automáticos para as autoridades responsáveis. Tais tecnologias podem auxiliar no combate e na prevenção de tiroteios em massa, como vem ocorrendo em diversos estados dos Estados Unidos e em alguns casos no Brasil.

No contexto de IA em segurança pública, merecem destaque os sistemas de reconhecimento facial para identificar indivíduos foragidos ou comportamentos criminosos em locais públicos. O reconhecimento facial é uma tecnologia de identificação biométrica que utiliza algoritmos de IA para analisar detalhadamente uma imagem capturada por uma câmera, definindo um padrão individual para os rostos verificados. Esta tecnologia permite a criação de um banco de dados com as informações extraídas acerca de traços específicos para produzir o chamado padrão facial, possibilitando a identificação das pessoas (COSTA & KREMER, 2022).

Oliveira (2021) observa que a necessidade do uso do reconhecimento facial advém do acelerado processo de crescimento urbano e populacional nas cidades pelo mundo. Nesse sentido, houve um aumento da demanda por um maior controle estatal, sendo comum que a gestão pública adote novas formas de vigilância sobre as pessoas. Não por acaso, a concepção das cidades inteligentes reflete o interesse estatal em tecnologias de comunicação e informação (TIC) e no processamento de bancos de dados pessoais massivos, tendo em vista a utilidade para o planejamento urbanístico (BARROS; VENTURINI, 2018; COSTA & KREMER, 2022).

Apesar dos casos que podem ser vistos como positivos para a segurança pública e investigação criminal, o uso de tecnologias de reconhecimento facial tem sido objeto de ampla discussão, especialmente em relação aos problemas associados a viés e discriminação que surgem, em muitos casos, devido a bases de dados de treinamento insuficientemente representativas (ELIAS, 2021; COSTA & KREMER, 2022). Embora sistemas de reconhecimento facial para segurança pública tenham sido empregados em inúmeras situações, inclusive no Brasil, os índices de falsas identificações positivas ou negativas suscitam preocupações. Possíveis erros utilizados para segurança pública podem representar constrangimentos, atribuição inverídica de antecedentes criminais a inocentes, prisões arbitrárias e violações de direitos fundamentais, como o direito à presunção de inocência e o princípio da não discriminação, acarretando prejuízos democráticos.

Outrossim, problemas relacionados a viés de gênero e de raça têm sido constatados em diversos casos de uso de sistemas de reconhecimento facial (SCHULER & MONTARDO, 2020). Tal noção fica clara no relatório do NIST<sup>1</sup> sobre questões demográficas em sistemas de reconhecimento facial. O relatório constatou que os falsos positivos são muito maiores na identificação de pessoas com traços africanos e asiáticos do que para traços europeus caucasianos. Ainda, a parcela de falsos positivos em mulheres também foi maior do que em homens. O problema reside no fato de que as máquinas utilizadas no reconhecimento facial refletem as percepções daqueles que as desenvolvem e do tratamento oferecido pelos bancos de dados que as alimentam.

Portanto, há uma grande probabilidade de erros como os supracitados se tornarem mais frequentes por meio do uso do reconhecimento facial. Isso ocorre devido a questões estruturais relacionadas à forma como a sociedade e o Estado interpretam quem são os indivíduos que devem ser alvo de vigilância e perseguição, ou seja, quem são as pessoas consideradas perigosas e que devem ser detidas. Desse modo, tais vieses podem colocar em risco a liberdade de pessoas inocentes quando são implantados por serviços de segurança pública para identificar criminosos (SCHULER & MONTARDO, 2020).

Schuler & Montardo (2020) apontam para uma tendência internacional ao banimento do uso de tecnologias de reconhecimento facial, especialmente nos Estados Unidos. Os autores apresentam diversas cidades americanas que seguem tal tendência, como São Francisco, Portland, Mineápolis, Cambridge, Oakland, Nova Orleans e dezenas de outros municípios. Além disso, há recomendações do AI Act, promovida pela Autoridade Europeia de Proteção de Dados, em prol do banimento de tecnologias de reconhecimento facial em todo o bloco europeu.

Brasil (2020) apresenta que o emprego do reconhecimento facial para fins de vigilância sempre afeta negativamente o princípio da presunção de inocência, mesmo que operasse sem vieses. Isso ocorre porque a utilização desse mecanismo subverte a lógica do sistema legal em um Estado Democrático de Direito, no qual toda investigação que afete direitos fundamentais deve derivar de uma suspeita fundamentada. Enquanto o reconhecimento facial implica na vigilância prévia de todos

---

<sup>1</sup> Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>.

os cidadãos de forma generalizada, ubíqua e remota, ou seja, sem o conhecimento e consentimento do cidadão.

Schuler & Montardo (2020) indicam a falta de transparência no cenário brasileiro em relação aos contratos de fornecimento desses sistemas, além da falta de conhecimento acerca dos critérios utilizados para reconhecimento de padrões faciais por essa tecnologia, ou como funcionam os *inputs* nos bancos de dados. Tais fatores são extremamente prejudiciais para a democracia, uma vez que ferem o princípio da transparência, o da não-discriminação, além de que podem afetar negativamente os direitos à intimidade, à privacidade e à proteção de dados pessoais (BRASIL, 2020).

A questão de fornecimento de sistemas de IA, não apenas para reconhecimento facial, por empresas estrangeiras traz implicações sociais, políticas e econômicas para a sociedade brasileira. Morozov (2018), ao tratar da influência do domínio dos monopólios digitais por grandes empresas de tecnologia na política e na economia da sociedade, o autor estabelece que a propagação da ideologia dos países dominantes para as nações pobres é uma importante arma de dominação. Com isso, os países com soberania econômica e soberania tecnológica, como é o caso dos Estados Unidos, criam grau de dependência da administração pública brasileira com suas empresas estrangeiras para contratação de mecanismos de IA, detentoras do armazenamento e manejo de diversos dados pessoais. Isso enfraquece a soberania nacional brasileira, tendo em vista que essas empresas refletem e defendem, direta ou indiretamente, os interesses políticos e econômicos das potências mundiais, dos seus proprietários e acionistas (MOROZOV, 2018).

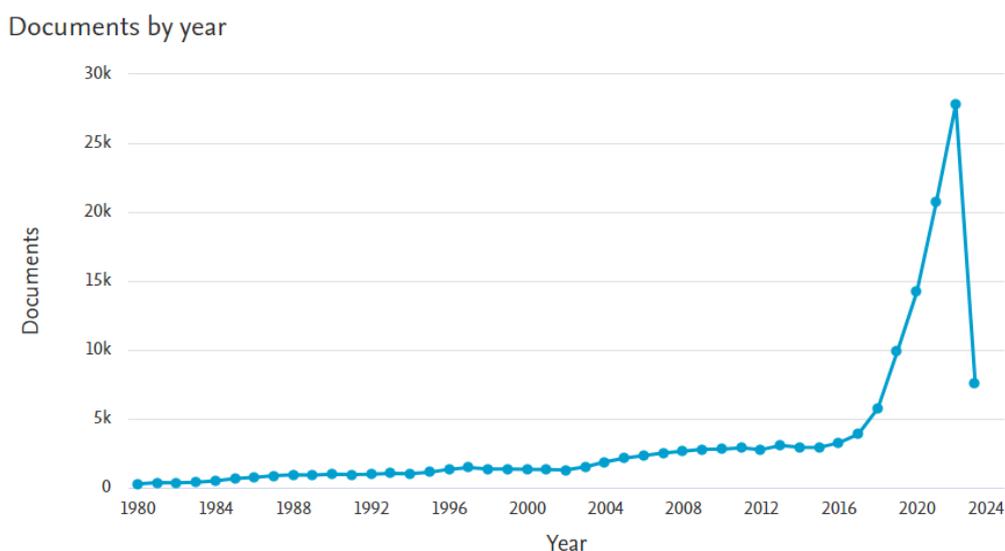
Cabe ressaltar que a aplicação de tecnologias de Inteligência Artificial, quando focada na Segurança Pública, geralmente requer o processamento de vastas quantidades de dados para o treinamento do modelo, promovendo assim a criação e/ou a disponibilização de extensos bancos de dados pessoais (BRASIL, 2020). Esse processo pode resultar em potenciais danos à privacidade dos cidadãos. Ainda que as atividades de segurança pública estejam excluídas da aplicação da Lei Geral de Proteção de Dados (LGPD), precisam estar em adequação aos seus princípios. É crucial que as pessoas sejam transparentemente informadas sobre como os dados foram armazenados para a criação de uma ferramenta utilizada por um órgão governamental específico (BRASIL, 2020).

## 3 Metodologia

### 3.1 Caracterização da pesquisa

Quanto aos objetivos, a pesquisa desenvolvida é caracterizada como descritiva e exploratória. Para Triviños (1987), a pesquisa descritiva pretende descrever os fatos e fenômenos de determinada realidade, buscando caracterizar o objeto de análise. Assim, a pesquisa é descritiva porque propõe em seus objetivos oferecer um panorama explicativo dos casos de iniciativas de IA que foram implementados no governo executivo federal até setembro de 2023, descrevendo-as e caracterizando-as. Ademais, é exploratória em razão da baixa disponibilidade de informações acerca das iniciativas, bem como pelo uso de IA no setor público se tratar de um tema relativamente recente e em crescimento. Apenas nos últimos 5 anos, foram publicados mais de 78 mil textos científicos que incluíam “AI” ou “Artificial Intelligence” nas suas palavras-chave publicados na base científica *Scopus*, chegando a um pico recente de mais de 25 mil artigos publicados no ano de 2022 (Figura 1).

**Figura 1** - Número de textos com palavras-chave relacionadas à IA publicados na base Scopus por ano



Fonte: Elaboração própria com base nos dados da Scopus, 2023.

Segundo Triviños (1987), estudos exploratórios permitem ao pesquisador aumentar sua experiência em torno de determinada questão. Ainda, Gil (2008) indica que esse tipo de pesquisa é realizado quando o tema escolhido é pouco explorado, e é desenvolvida com o objetivo de proporcionar visão geral, de tipo aproximativo, acerca de determinado fato. Desse modo, tal estudo é exploratório, visto que pretende encontrar as iniciativas necessárias para permitir a análise proposta acerca de seus potenciais riscos e benefícios à democracia.

A abordagem fundamental da pesquisa pode ser entendida como mista, apresentando características de uma abordagem quantitativa e qualitativa. A pesquisa quantitativa tem como cerne a objetividade, seus resultados podem ser quantificados e expressados numa linguagem numérica ou matemática, recorre a instrumentos padronizados e suas amostras geralmente são consideradas representativas (FONSECA, 2002).

Já a investigação qualitativa é um tipo de estudo descritivo que se concentra principalmente no significado, na interpretação e na compreensão dos fenômenos (TRIVIÑOS, 1987). Ela enfatiza a subjetividade e a flexibilidade do estudo, reconhecendo também a conexão intrínseca entre o comportamento das variáveis e o contexto em que se inserem. Fonseca (2002, p. 20) indica que “a utilização conjunta da pesquisa qualitativa e quantitativa permite recolher mais informações do que se poderia conseguir isoladamente”.

A pesquisa também recorreu à revisão bibliográfica para compreensão acerca dos potenciais riscos e benefícios democráticos a partir do uso de artefatos tecnológicos que, sem a pretensão de esgotar o conhecimento acerca do assunto, pretendeu oferecer um panorama acerca do tema e a perspectiva escolhida como recorte para análise.

Quanto à natureza dos dados trabalhados, a pesquisa obteve dados primários acerca das iniciativas de IA implementadas num panorama temporal mais recente, e recorreu a dados secundários acerca de iniciativas já abordadas em documentos oficiais, artigos científicos, *sites* de organizações da sociedade civil, em especial da Transparência Brasil, e *sites* governamentais.

### **3.2 Procedimentos de coleta dos dados da pesquisa**

Para alcançar os objetivos propostos, o presente estudo utilizou a pesquisa documental e a pesquisa bibliográfica como métodos de sistematização de dados. Resumidamente, a pesquisa documental utiliza fontes de dados contidos em documentos públicos ou privados, compostos por fontes mais diversificadas e dispersas sem tratamento analítico, dentre estas: tabelas estatísticas, jornais, revistas, documentos oficiais, entre outros que possibilitam o acesso à informação com custo reduzido e com ausência de constrangimento de indivíduos (GIL, 2010). Já a pesquisa bibliográfica é desenvolvida a partir de material já elaborado, composto principalmente de livros e artigos científicos. Gil (2010) aponta como a principal vantagem da pesquisa bibliográfica a possibilidade de oferecer a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia se pesquisar diretamente.

No caso do presente estudo, a pesquisa documental realizada se deu com base em documentos oficiais disponibilizados em meio eletrônico pelo Governo Federal brasileiro por meio dos *sites* dos órgãos públicos. A pesquisa bibliográfica pretende complementar os achados da pesquisa documental, bem como fornecer insumos para estudo de possíveis riscos e benefícios democráticos oferecidos pelas iniciativas mapeadas.

Um dos procedimentos de coleta de dados consistia em enviar pedidos de acesso à informação e busca em transparência ativa ao Ministério da Ciência, Tecnologia e Inovação em relação a dados referentes ao monitoramento das iniciativas de IA realizado pelo órgão. O pedido de acesso à informação foi realizado com base no disposto pela EBIA, a qual estabelece como ação estratégica “implementar recursos de Inteligência Artificial em, no mínimo, 12 serviços públicos federais até 2022” (BRASIL, 2021b, p. 44). Assim, o pedido foi feito ao MCTI com o intento de receber informações acerca das iniciativas mapeadas até setembro de 2023. Contudo, o órgão não forneceu tais informações, o que prejudicou um dos procedimentos de coleta de dados da presente pesquisa.

Por fim, após mapear as iniciativas de IA com base nos procedimentos supracitados, foram enviados questionários aos órgãos do Poder Federal que apresentem iniciativas na área de Segurança Pública e que fazem parte da lista de órgãos federais do Sistema Eletrônico de Informações ao Cidadão (e-SIC) em busca de transparência ativa. Foi enviado, também, um questionário ao Instituto Glória, vide apêndice B, com o objetivo de obter informações mais profundas acerca da

ferramenta. Não houve resposta do Instituto, porém, o que tornou prejudicada a análise mais aprofundada dessa ferramenta.

As perguntas enviadas nos questionários foram desenvolvidas com base no Referencial Teórico a fim de compreender, no geral: i: as características das ferramentas; ii: seus objetivos; iii) qual o público-alvo da ferramenta (interno ou externo); iv) se as ferramentas promoveram aprimoramento dos processos internos em questão de tempo e economia de recursos; v) se as ferramentas foram desenvolvidas no setor público ou compradas prontas; vi) quais as variáveis de entrada e de saída das ferramentas; vii) as ferramentas possibilitaram uma melhor entrega de serviços aos cidadãos; viii) se há realizações periódicas de auditorias do funcionamento do algoritmo por especialistas externos ao órgão público; ix) se as ferramentas seguem as recomendações já existentes de desenvolvimento, como as recomendações da Estratégia Brasileira de Inteligência Artificial; x) se as ferramentas apresentam impacto no processo de decisão; xi) se no desenvolvimento e/ou implementação das ferramentas, foi considerada a obrigatoriedade de revisão humana das decisões automatizadas; e xii) se no desenvolvimento e/ou implementação das ferramentas, foram considerados possíveis vieses em seu desempenho.

As perguntas enviadas variaram em função da variedade de ferramentas utilizadas pelos mesmos órgãos, como é o caso do Conselho Administrativo de Defesa Econômica - Cade, da Polícia Federal e do Ministério da Justiça e Segurança Pública, bem como por causa da diferença da natureza das ferramentas, como é o caso do Robô Glória.

### **3.3 A amostra**

A pesquisa consistiu em investigar as iniciativas de IA dos órgãos do governo federal os quais apresentam relação com a área de Segurança Pública, sendo que foram encontradas mais de uma iniciativa por órgão público, além de uma iniciativa de IA orientadas para segurança pública desenvolvidas pela sociedade civil em parceria com o governo federal. A amostra envolveu as treze (13) iniciativas do governo federal mapeadas voltadas para a área de Segurança Pública, e uma iniciativa da sociedade civil. Dentre as iniciativas governamentais, pode-se apontar a

A.I Desk; a D.E.I.A - Defesa Econômica com Inteligência Artificial; o Databricks; o Delphos; o LED; o Nudetective; o PalasNet; o Projeto Cérebro; o SINESP Big Data; o Sistema Alerta Brasil; o Sistema Córtex; a Solução Automatizada de Identificação Biométrica (ABIS); e a Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa. Já a iniciativa da sociedade civil se refere ao Robô Glória, uma interface de comunicação com mulheres e meninas vítimas de violência, focada no apoio e na busca de soluções para cada caso.

### 3.4 Instrumentos de coleta e análise de dados

Como instrumentos de coleta de dados, foram utilizados: coleta manual das iniciativas em meio eletrônico; uso de um algoritmo, que foi desenvolvido pelo grupo de pesquisa do qual a autora participa (GERIS, UnB), para busca automatizada e mais abrangente de notícias relacionadas à IA utilizados pelo setor público e pela sociedade civil em parceria com o setor público; questionários enviados aos órgãos do Executivo Federal com iniciativas em Segurança Pública; questionário enviado ao Ministério de Ciência, Tecnologia e Inovação (MCTI), vide apêndice A; e questionário enviado ao Instituto Glória, vide apêndice B.

Para o desenvolvimento do algoritmo de busca automatizada, foi empregue a linguagem de programação Python, a qual é vastamente utilizada no contexto da Ciência/Análise de dados. Utilizou-se o *script* Python “Buscador” para coletar, no Google, links que incluíam palavras-chave relacionadas ao tema<sup>2</sup>. A busca foi filtrada para exibir apenas resultados presentes em sites governamentais brasileiros terminados em “.gov.br”, “.leg.br”, “.jus.br” e “.mp.br”, os quais são domínios públicos definidos em convenções internacionais. Inicialmente, foram obtidos um total de 13.303 links.

---

<sup>2</sup> Os termos de busca foram “algoritmo and “segurança pública” “machine learning” and “segurança pública” “solução automatizada” and “segurança pública” “solução automatizada” and “criminalidade” “solução automatizada” and “criminalidade” and ferramenta “inteligência artificial” and “criminalidade” “inteligência artificial” and “policiamento” “inteligência artificial” and “criminalidade” and ferramenta “inteligência artificial” and “segurança pública” “inteligência artificial” and “segurança pública” and “sistema” “inteligência artificial” and ferramenta and “segurança pública” “inteligência artificial” and “segurança pública” and iniciativa “segurança pública” and “reconhecimento facial” “segurança pública” and “biometria” “segurança pública” and “biometria” and “inteligência artificial” “segurança pública” and geolocalização and “inteligência artificial” “segurança pública” and videomonitoramento “segurança pública” and videomonitoramento and “inteligência artificial” “inteligência artificial” and “violência”.

Subsequentemente, utilizou-se o código Python denominado "segmentador" para refinar os *links* com base no conteúdo inicial recuperado pela pesquisa. Nessa etapa, foram empregadas as seguintes palavras-chave: ferramenta, sistema, robô, bot, chatbot, iniciativa, programa e projeto. Tal filtragem resultou em 2.696 registros. Após uma análise preliminar dos *links*, tomou-se a decisão de excluir da lista aqueles que direcionavam para arquivos com extensão pdf, uma vez que muitos deles estavam relacionados a páginas de diário oficial e a outros conteúdos de menor relevância. Isso culminou em um total de 1.703 links. Em seguida, procedeu-se à implementação do código Python "*scraper*" para a extração do conteúdo desses links. Com base no conteúdo dos links, uma amostra de 182 registros foi selecionada e esses foram rotulados como "relevantes", enquanto outra amostra de 182 registros rotulados como "não relevantes", totalizando 364 registros (21,37% do total).

A próxima etapa envolveu a implementação do código Python "estimador". Este código aplicou o algoritmo de aprendizado supervisionado "Regressão Logística". Os dados rotulados, totalizando 364 registros, foram usados para treinar um modelo de classificação. Posteriormente, os dados não rotulados, que somavam 1.339 registros, foram apresentados ao modelo para que ele fizesse inferências sobre o nível de relevância de cada página no contexto da pesquisa. Os registros foram, então, classificados em ordem, do mais relevante ao menos relevante, selecionando-se para análise individual os 25% mais relevantes, totalizando 379 registros.

Foram realizadas análises qualitativas dos 379 registros, averiguando os instrumentos algorítmicos que estão sendo, de fato, implementados no campo da segurança pública por organizações governamentais brasileiras. Foi possível obter o total de trinta e sete (37) instrumentos que fazem uso de recursos de IA nos governos municipais, estaduais e no governo federal no campo da segurança pública no país. Com isso, chegou-se ao total de 11 (onze) instrumentos que fazem uso de recursos de IA no governo federal no campo da segurança pública no Brasil, além de um instrumento desenvolvido pela sociedade civil em parceria com o governo federal. No entanto, é importante destacar que esses números representam apenas uma fração da quantidade efetivamente utilizada. Cabe destacar que, entre os 11 instrumentos encontrados por meio do algoritmo, dois já haviam sido localizados por meio de coleta manual em meio eletrônico.

Para a análise dos dados, escolheu-se a triangulação dos dados coletados por métodos distintos, tendo em vista que foram utilizados dados de distintas fontes com

diferentes pontos de vistas (MINAYO, 2010). O objetivo dessa escolha é oferecer o panorama mais abrangente possível acerca das iniciativas e permitir que a análise das iniciativas seja feita por uma perspectiva diversa. Trata-se, assim, de construir uma maior confiabilidade para os resultados da pesquisa.

## 4 Análise dos Dados Coletados

Nesta seção foram analisadas as iniciativas de Inteligência Artificial voltadas para a área de Segurança Pública na esfera federal, bem como a iniciativa desenvolvida pela sociedade civil em parceria com o governo federal.

### 4.1 Descrição e caracterização de iniciativas de IA do Governo Federal orientadas para Segurança Pública

No que tange às iniciativas de Inteligência Artificial voltadas para a área de Segurança Pública utilizadas por órgãos do Governo Federal, foram mapeadas treze (13) no total. Duas iniciativas foram localizadas por meio de coleta manual em meio eletrônico, cujas fontes basearam-se em pesquisas bibliográficas. Onze iniciativas foram encontradas por meio do algoritmo para busca automatizada desenvolvido pelo grupo de pesquisa do qual a autora faz parte (GERIS, UnB), incluindo as duas localizadas primeiramente por meio de coleta manual. Por fim, informações acerca de outras duas iniciativas foram fornecidas pelos pedidos de acesso à informação em busca de transparência ativa feitos aos órgãos de segurança pública do governo federal por meio da plataforma Fala.br, uma plataforma integrada de ouvidoria e acesso à informação, recurso da Controladoria-Geral da União. A Tabela 1 a seguir explicita quais foram os métodos utilizados para encontrar cada iniciativa, bem como apresenta as iniciativas e seus órgãos implementadores.

**Tabela 1** - Métodos utilizados e órgãos implementadores para cada iniciativa mapeada

Iniciativa	Método Utilizado para Localizar a Ferramenta	Órgão Implementador
A.I Desk	Algoritmo do grupo GERIS	Polícia Federal - PF
D.E.I.A. - Defesa Econômica com Inteligência Artificial.	Pedido de acesso à informação por meio da plataforma Fala.br	Conselho Administrativo de Defesa Econômica - Cade
DataBricks	Pedido de acesso à informação por meio da plataforma Fala.br	Ministério da Justiça e Segurança Pública - MJSP

Delphos	Algoritmo do grupo GERIS	Polícia Federal - PF
Localizador de Evidências Digitais	Algoritmo do grupo GERIS	Polícia Federal - PF
NuDetective	Algoritmo do grupo GERIS	Polícia Federal - PF
PalasNET	Pesquisa Bibliográfica	Departamento Penitenciário Nacional
Projeto Cérebro	Algoritmo do grupo GERIS	Conselho Administrativo de Defesa Econômica - Cade
Sinesp Big Data	Algoritmo do grupo GERIS	Ministério da Justiça e Segurança Pública - MJSP
Sistema Alerta Brasil	Algoritmo do grupo GERIS	Departamento da Polícia Rodoviária Federal
Sistema Córtex	Algoritmo do grupo GERIS	Ministério da Justiça e Segurança Pública - MJSP
Solução Automatizada de Identificação Biométrica (ABIS)	Pesquisa Bibliográfica	Polícia Federal - PF
Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa	Algoritmo do grupo GERIS	Comissão de Valores Imobiliários (CVM)

Fonte: Elaboração própria, 2023.

Segue abaixo a descrição e caracterização de cada uma das ferramentas.

## A.I Desk

Ao ser questionada acerca da ferramenta por meio de solicitação de acesso à informação na plataforma Fala.br, a Polícia Federal informou não dispor de conhecimento acerca de uma ferramenta chamada A.I Desk, apesar dos indícios encontrados que apontam para sua existência. A ferramenta está presente no *Catálogo de Uso de Inteligência Artificial por Órgãos Governamentais* disponibilizado pelo Transparência Brasil, o qual disponibiliza informações fornecidas pela Polícia Federal acerca do A.I Desk<sup>3</sup>, um sistema baseado em inteligência artificial utilizado

<sup>3</sup> Dados disponibilizados em “AI.desk,” *Catálogo de Uso de Inteligência Artificial por Órgãos Governamentais*, acesso em 26 de outubro de 2023, <https://catalogoia.omeka.net/items/show/33>.

pela Polícia Federal. Ainda, foi possível encontrar o artigo *A Benchmark Methodology for Child Pornography Detection*, produzido pelo Perito Criminal Federal e seus colaboradores no desenvolvimento da ferramenta A.I Desk. No artigo, publicado em 2018, os autores informaram que a ferramenta era utilizada pela Polícia Federal brasileira (MACEDO, COSTA & DOS SANTOS, 2018). Ademais, foi possível identificar a existência do Termo de Referência relativo à Cotação Eletrônica 29/2019, no qual é tratada a compra de placa de vídeo pela Polícia Federal do Rio Grande do Sul com o objetivo de viabilizar a utilização de sistema de inteligência artificial denominado A.I Desk. Pode ser que a ferramenta não esteja mais sendo utilizada pela Polícia Federal atualmente, mas, para garantir transparência pública, era imprescindível que o órgão ao menos prestasse tal informação. Isso potencializa o problema de opacidade algorítmica trazida por Fornasier (2021), e aponta para o que se detectou neste estudo como opacidade na gestão, na qual nem o próprio órgão responsável pela implementação da ferramenta é capaz de fornecer dados relativos a ela.

Apesar de não ter sido reconhecida pela PF na solicitação de acesso à informação, optou-se por tratar da ferramenta em razão das evidências que apontam para sua existência. Trata-se de um sistema concebido no setor público, desenvolvido pelo Perito Criminal Federal (PCF) João José de Macedo Neto e colaboradores, e tem como objetivos automatizar as análises de pornografia infantil em arquivos eletrônico-digitais de imagens ao auxiliar na identificação de rostos, classificar rostos em grupos de idades e identificar objetos em cenas. Assim, a ferramenta propõe-se a automatizar o processamento de arquivos eletrônico-digitais de imagens com o intuito de determinar a presença de pornografia infantil.<sup>4</sup>

O sistema é voltado para a gestão interna, e apresenta como categorias de aplicação o reconhecimento facial e a classificação de imagens, e seu modelo estatístico é baseado em redes neurais convolucionais<sup>5</sup>. Seus *outputs*, ou saídas, consistem em estimar a probabilidade de determinada imagem conter nudez, estimar

---

<sup>4</sup> Informações disponibilizadas no Termo de Referência relativo à Cotação Eletrônica 29/2019 - Aquisição de Placas de Vídeo no estado do Rio Grande do Sul, acesso em: 20 de out. 2023. Disponível em <https://www.gov.br/pf/pt-br/assuntos/licitacoes/2019/rio-grande-do-sul/cotacoes-eletronicas/cotacao-eletronica-29-2019-aquisicao-de-placas-de-video/termo-de-referencia.pdf/view>

<sup>5</sup> Dados presentes no artigo *A Benchmark Methodology for Child Pornography Detection*, produzido pelo Perito Criminal Federal e seus colaboradores no desenvolvimento da ferramenta. O artigo apresenta a pesquisa feita para a criação da ferramenta, contando com diversas informações acerca de seu desenvolvimento.

a faixa de idade dos rostos identificados e estabelecer a categoria das imagens (MACEDO, COSTA & DOS SANTOS, 2018). Quanto à sua influência no processo de tomada de decisão, foi observado que o instrumento apoia o processo de tomada de decisão ao fazer diagnósticos, mas não sugere ações.<sup>6</sup>

### **D.E.I.A. - Defesa Econômica com Inteligência Artificial**

No seu Planejamento Estratégico 2021/2024, o Conselho Administrativo de Defesa Econômica - Cade possui o projeto chamado D.E.I.A. - Defesa Econômica com Inteligência Artificial. A ferramenta propõe viabilizar a instrumentalização dos processos em trâmite na autarquia, consultando bases de dados governamentais já existentes. A intenção é que a ferramenta auxilie na geração de minutas de documentos que fazem parte do processo de análise, como por exemplo, pareceres, editais etc. A ferramenta também conta com técnicas digitais para facilitar a análise de condutas anticompetitivas e atos de concentração, além de automatizar alguns processos de trabalho que eram realizados de forma manual.<sup>7</sup> As tarefas de IA a serem realizadas consistem no reconhecimento das entidades nomeadas, na relação ontológica de termos, na sumarização de documentos, na construção de nuvens de palavras, na análise estatística de documentos e na elaboração de minuta de documentos.

Segundo informações do órgão implementador, o Cade, a ferramenta foca em atividades de Processamento de Linguagem Natural, e o seu objetivo é interpretar a linguagem humana, desde métodos estatísticos e de *machine learning* a abordagens algorítmicas e baseadas em regras<sup>8</sup>. Em relação às atividades desempenhadas, o órgão apontou para: elaboração de minutas de documentos, elaboração para ementas e resumos de documentos, reconhecimento de pessoas físicas e jurídicas em documentos e reconhecimento de legislações e jurisprudências. Trata-se de uma inovação tecnológica desenvolvida pelo próprio órgão público e o público-alvo da

---

<sup>6</sup> Dados disponibilizados em "AI.desk," Catálogo de Uso de Inteligência Artificial por Órgãos Governamentais, acesso em 26 de outubro de 2023, <https://catalogoia.omeka.net/items/show/33>.

<sup>7</sup> Informação obtida por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br com resposta obtida no dia 20 de novembro de 2023.

<sup>8</sup> Informação obtida por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br com resposta obtida no dia 26 de setembro de 2023.

ferramenta é interno. Para mais, o órgão informou que as ações realizadas pela ferramenta contam com revisão humana.

## DataBricks

Ferramenta do Ministério da Justiça e Segurança Pública, o Databricks refere-se a um *software* utilizado para processamento, transformação e exploração de grandes volumes de dados, ou *Big Data*, de forma distribuída. Segundo informações disponibilizadas pelo órgão, tal ferramenta utiliza técnicas de *machine learning*. O órgão informou que a ferramenta possui funções de reconhecimento facial, *chatbots*, classificação de imagens, sistema de filtragem de pedidos dos cidadãos, estimativa de risco e sistemas de recomendação. Contudo, o MJSP ainda não utiliza o Databricks de forma completa para tais finalidades, e não informou quais seriam as categorias de aplicação utilizadas até o momento de realização desta pesquisa<sup>9</sup>.

Ainda com base nas informações disponibilizadas pelo órgão, o *software* permitiu que os servidores obtivessem acesso aos dados consumidos para criação de painéis de *Business Intelligence* (BI) e para o consumo de *Application Programming Interface* (API). Segundo Botelho-Francisco e Orlando (2015), as APIs são utilizadas na programação de *software* para facilitar a integração de sistemas, o compartilhamento de dados e funcionalidades entre diferentes aplicativos e serviços, mesmo que esses utilizem diferentes linguagens de programação<sup>10</sup>. Já os painéis de BI são ferramentas de visualização de dados que oferecem uma síntese de informações relevantes para uma organização, permitindo que os usuários tomem decisões informadas com base em dados cujas análises totais seriam muito complexas (GONÇALVES, 2017).

---

<sup>9</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

<sup>10</sup> Definição dos autores: “Uma API reúne um conjunto de estruturas de dados, funções e protocolos que permitem que aplicações se comuniquem entre si, sem intervenção humana. Em contraponto, uma Interface de Usuário (UI – User Interface) permite que um usuário interaja com uma aplicação através de linha de comando (CLI – Command Line Interface), elementos gráficos (GUI – Graphical User Interface), voz (VUI – Voice user Interface) etc. Uma das grandes vantagens do uso de APIs é que as particularidades técnicas tanto dos provedores de serviço quanto dos consumidores são abstraídas. Em termos mais concretos, isso significa que um provedor de serviço codificado em uma linguagem de programação como C++ pode ser acessado com sucesso por um CMS codificado na linguagem PHP” (BOTELHO-FRANCISCO & ORLANDO, 2015, p. 46).

Não se trata de uma ferramenta desenvolvida no setor público, o órgão informou que a ferramenta foi comprada por uma empresa de nome homônimo, a Databricks. Por meio do *site* oficial da empresa<sup>11</sup>, é possível verificar que a ferramenta já foi comercializada para órgãos governamentais dos Estados Unidos, a exemplo da Agência Nacional de Informação Geoespacial, da sua Força Aérea e do Departamento de Segurança Interna dos Estados Unidos. A empresa informa que a ferramenta foi utilizada por tais órgãos para diversas funções, como análise preditiva, detecção e prevenção de atividades criminosas<sup>12</sup>. Neste ponto, é possível estabelecer relação com a tese de Morozov (2018), que trata da dependência tecnológica entre países mais subdesenvolvidos, como o Brasil, com países como os Estados Unidos, que dispõe de soberania econômica e, assim, tecnológica.

No caso do MJSP, o órgão indica que a ferramenta é utilizada apenas para cruzamento, consulta e acesso a dados, além da automatização do processo de atualização desses dados. Não foi informado, entretanto, o contexto de utilização de tais dados, nem como eles são tratados. Por fim, o órgão informa que, no que se refere ao processo de tomada de decisão, a ferramenta efetua diagnósticos mediante programação prévia, mas no contexto atual não sugere ações.

## Delphos

Segundo informações disponibilizadas pelo órgão implementador<sup>13</sup>, o Delphos é uma plataforma concebida para auxiliar peritos em suas atividades, composta por vários módulos destinados à indexação de documentos, registros periciais diversos (como veículos e papel-moeda), tipologias e informações relacionadas ao ouro (incluindo um banco de perfis auríferos e cruzamento de dados de mineração). É importante destacar que o Delphos incorpora uma variedade de tecnologias e técnicas em seus diferentes módulos, sendo que somente alguns deles fazem uso de inteligência artificial, e são inseridos na categoria de estimativa de risco (detecção de fraudes). Por fim, os *outputs*, ou saídas da ferramenta, referem-se ao reconhecimento

---

<sup>11</sup> Disponível em <https://www.databricks.com/br>. Acesso em: 20 de out. 2023).

<sup>12</sup> Dado disponível em <https://www.databricks.com/wp-content/uploads/2021/04/Federal-Government-Solution-Sheet-2.pdf>. Acesso em : 20 de out. 2023).

<sup>13</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

de entidades (nomes de pessoas, empresas, endereços, valores, e-mails, números de telefone etc.).

O principal objetivo da ferramenta é fornecer, de maneira modular, uma interface intuitiva que agregue valor às atividades periciais, ao mesmo tempo que, em segundo plano, ofereça suporte às demais atividades da Polícia Federal que possam se beneficiar de suas funcionalidades. A plataforma utilizada para cruzamento de bases de dados é baseada em *software* livre e foi desenvolvida pelos peritos no âmbito da Diretoria Técnico-Científica da Polícia Federal. O modelo estatístico por ela utilizado é o de regressão linear e processamento de linguagem natural. No que se refere ao seu papel no processo decisório, o órgão indicou que a ferramenta faz diagnósticos, mas não sugere ações. A ferramenta é alimentada por dados abertos disponibilizados por portais da transparência.<sup>14</sup>

### **Localizador de Evidências Digitais (LED)**

O Localizador de Evidências Digitais (LED) é uma ferramenta para triagem em mídias de armazenamento computacional, arquivos possivelmente relacionados à pornografia infantojuvenil que, dentre suas diversas funcionalidades, utiliza um algoritmo baseado em aprendizado de máquina para classificação de imagens e vídeos.

Segundo dados disponibilizados pelo órgão implementador<sup>15</sup>, o objetivo do LED é prestar suporte ao cumprimento de mandados de busca e apreensão em locais relacionados à investigação de crimes previstos no Art. 241 do Estatuto da Criança e do Adolescente (ECA). Nessas instâncias, o instrumento fica encarregado de identificar possíveis arquivos de pornografia infantil que possam estar armazenados em dispositivos computacionais, como notebooks, discos rígidos portáteis, pen drives, entre outros.

Nesse panorama, a ferramenta auxilia o policial ao varrer uma vasta quantidade de arquivos presentes nesses dispositivos e identificar arquivos que possuam características suspeitas e uma alta probabilidade de estarem relacionados aos delitos

---

<sup>14</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

<sup>15</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

sob investigação. Dentre os critérios utilizados na análise, incluem-se a detecção de termos específicos nos nomes dos arquivos, a identificação de arquivos característicos (como os associados a programas de compartilhamento de arquivos em redes P2P), a comparação com uma base de dados contendo cerca de 3,7 milhões de arquivos de pornografia infantil previamente registrados em casos anteriores, bem como a identificação de imagens e vídeos que contenham possível conteúdo de nudez.<sup>16</sup>

Em relação às variáveis de entrada do algoritmo, segundo a Diretoria Técnico-Científica da Polícia Federal, o instrumento utiliza basicamente as propriedades (texto, tamanho, pasta etc.) e o conteúdo dos arquivos para emitir os alertas. Em relação ao algoritmo de detecção de nudez, ela utiliza como *features* a intensidade luminosa, tons, texturas, entre outras características das imagens ou frames dos vídeos, indicados em diversas regiões das imagens. Já as saídas do algoritmo consistem na apresentação de uma pontuação de 1 a 1000, permitindo ordenação, destacando as imagens e vídeos com maior probabilidade de conter nudez.<sup>17</sup>

Trata-se de uma ferramenta desenvolvida internamente, pelo Perito Criminal Federal Wladimir Luiz Caldas Leite, e foi aprimorada ao longo dos últimos 13 anos. Em relação ao modelo estatístico utilizado pelo algoritmo na função de detecção de imagens e vídeos com possível nudez, o órgão informa que se trata de um classificador binário baseado em conjunto de árvores de decisão aleatórias (*Random Forests*).

No que tange ao seu grau de apoio no processo de decisão, o órgão informou que a ferramenta apenas emite alertas para possíveis arquivos relevantes. Cabe ao policial que está analisando os alertas identificar os arquivos de efetivo interesse e tomar as devidas ações, tais como apreender ou não o equipamento, efetuar prisão em flagrante etc.<sup>18</sup>

## **NuDetective**

---

<sup>16</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

<sup>17</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

<sup>18</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

O NuDetective é um *software* baseado em algoritmos que classifica arquivos e, em especial, fotos e vídeos, como suspeitos ou não de ter relacionamento com abuso sexual de crianças e adolescentes. Outrossim, identifica arquivos e diretórios arquivos armazenados em computadores, HDs, pen drives, cartões de memória que tenham, em seu nome, palavras-chaves suspeitas de estarem relacionadas a abuso sexual de crianças, além de aplicativos suspeitos de celulares Android<sup>19</sup>.

O *software*, ao analisar os pixels de todas as imagens contidas no aparelho investigado para determinar quais deles são de cor de pele, incluindo dos tons mais retintos aos mais claros, define se uma foto é ou não suspeita. Com relação aos vídeos, é utilizado um cálculo estatístico. Também identifica arquivos e diretórios que tenham, em seu nome, palavras-chaves suspeitas de estarem relacionadas a abuso sexual de crianças. E, por fim, compara os valores *hashes* criptográficos de bancos de dados de arquivos relacionados a abuso de crianças com arquivos identificados no computador ou celular suspeito.<sup>20</sup>

Trata-se de um instrumento que foi desenvolvido internamente pelos peritos criminais federais (PCFs) Mateus de Castro Polastro e Pedro Monteiro da Silva Eleutério e cedida à PF e a outras forças da lei e universidades no Brasil e no mundo. A ferramenta foi desenvolvida em 2010 e vem sendo desenvolvida desde então, sendo que sua versão mais recente, a 4.0, foi lançada em 2021 (SILVA e POLASTRO, 2014). Ainda, em relação ao seu papel no processo de tomada de decisão, a Diretoria Técnico-Científica da Polícia Federal apontou que a ferramenta faz diagnósticos para serem analisados mais profundamente pelo usuário. Ou seja, a ferramenta, em si, não toma decisões.<sup>21</sup>

## PalasNet

---

<sup>19</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

<sup>20</sup> Os algoritmos estão detalhados nos seguintes artigos: - POLASTRO, MC. ; ELEUTÉRIO, PMS. - NuDetective: a Forensic Tool to Help Combat Child Pornography through Automatic Nudity Detection. Proceedings of Twenty-First International Workshop on Database and Expert Systems Applications (DEXA), v. 2010, p. 349- 353, Bilbao/Espanha. Ago/2010. - ELEUTÉRIO, PMS. ; POLASTRO, MC. - An Adaptive Sampling Strategy for Automatic Detection of Child Pornographic Videos. Proceeding of the 7th International Conference on Forensic Computer Science - ICoFCS 2012, ABEAT (ed.), ISBN 978-85-65069-08-3 - p. 12-19, Brasília/DF. Set/2012.

<sup>21</sup> Dados obtidos por meio de pedido de acesso à informação feito pela autora por meio da plataforma Fala.br no dia 19 de setembro de 2023.

Ferramenta utilizada pelo Departamento Penitenciário Nacional, o PalasNet é descrito pela Diretoria De Inteligência Penitenciária como “[...] um sistema informático desenvolvido para o compartilhamento de dados restritos entre as agências de Inteligência Penitenciária e de Segurança Pública” (PENITENCIÁRIA, 2022, p. 288). Brasil (2020) aponta que, segundo informações obtidas com a PF, o sistema é utilizado para registro de informações das investigações e dispõe de técnicas de classificação de imagens, reconhecimento facial e perfil criminal. Na solicitação de acesso à informação realizada pela autora desta pesquisa, contudo, o órgão não mencionou reconhecimento facial como uma das categorias de aplicação da ferramenta. Tal elemento também aponta para a opacidade da gestão, como foi observado na ferramenta A.I Desk.

Ainda de acordo com o relatório de Brasil (2020), um banco de dados criminais é utilizado como variável para treinamento do sistema. Em relação ao grau de apoio oferecido pela ferramenta, o órgão informa que a ferramenta faz diagnósticos, mas não sugere ações<sup>22</sup>. Trata-se de uma ferramenta desenvolvida pela equipe interna. Ademais, conforme Penitenciária (2022):

A plataforma possui interface amigável e intuitiva para o usuário, o que a qualifica como uma ferramenta com potencial para auxiliar em processos decisórios e prognósticos, produzir conhecimento, analisar perfis e contribuir noutras técnicas inerentes às atividades de inteligência. (PENITENCIÁRIA, 2022, p. 289, grifo nosso).

O uso do PalasNet é regulamentado pela Portaria GAB-DEPEN/DEPEN/MJSP nº 252, datada de 21 de setembro de 2021 (documento SEI! 15887479)<sup>23</sup>. Tal instrumento regulatório estabelece o Sistema PalasNet como um sistema informático colaborativo oficial destinado ao gerenciamento de informações restritas de interesse da Inteligência Penitenciária, dentro do escopo do Departamento Penitenciário Nacional (DEPEN) do Ministério da Justiça e Segurança Pública. Tal dispositivo, contudo, não menciona instrumentos regulatórios para uso de ferramentas de reconhecimento facial em seu escopo. O órgão alega acesso externo restrito a mais

<sup>22</sup> Dado disponível em: “PalasNET,” Catálogo de Uso de Inteligência Artificial por Órgãos Governamentais, acesso em 20 de outubro de 2023, <https://catalogoia.omeka.net/items/show/35>.

<sup>23</sup> Disponível em <http://dspace.mj.gov.br/handle/1/5473>. Acesso em: 25 de out. de 2023.

informações acerca da ferramenta em razão de cláusulas de Segredo de Justiça Criminal.<sup>24</sup>

## Projeto Cérebro

O Projeto Cérebro é uma iniciativa institucional da Superintendência-Geral do Conselho Administrativo de Defesa Econômica (SG/Cade), vinculado ao Ministério da Justiça e Segurança Pública (MJSP). Trata-se de um mecanismo utilizado para diagnosticar a probabilidade de ocorrência de acordo entre empresas licitantes. De acordo com curso disponibilizado pela ENAP<sup>25</sup>:

[...] O Projeto Cérebro consiste no desenvolvimento de técnicas e metodologias para detecção de cartéis a partir do uso de bases de dados sobre licitações públicas. Trata-se de uma estratégia proativa de investigação, que utiliza ferramentas de mineração de dados, testes estatísticos e algoritmos para permitir a identificação de indícios de atuação coordenada em compras públicas. (DE DEFESA ECONÔMICA, Conselho Administrativo et al, 2019, p. 9).

Trata-se de uma ferramenta desenvolvida no setor público, e a categoria de aplicação das ferramentas de mineração de dados, testes estatísticos e algoritmos é apontada pelo Cade como aplicação de análise de dados<sup>26</sup>. Os dados de entrada da ferramenta se referem a bases de dados públicas sobre licitações, e podem ser obtidas de fontes abertas como o Portal da Transparência do Governo Federal e o Comprasnet. Já os *outputs*, ou saídas, advindos de trilhas de investigação, protocolos de mineração e análise de dados (testes estatísticos e outros modelos) fornecem subsídios para apoiar a tomada de decisão no âmbito de processos de investigação de possíveis infrações à ordem econômica. Nesse sentido, a ferramenta apresenta impacto no processo de decisão, ao fazer diagnósticos, mas não sugerir ações. Ainda, o código do Cérebro é fechado, tendo em vista que contexto institucional no qual é

<sup>24</sup> Dado disponível em: “PalasNET,” Catálogo de Uso de Inteligência Artificial por Órgãos Governamentais, acesso em 20 de outubro de 2023, <https://catalogoia.omeka.net/items/show/35>.

<sup>25</sup> DE DEFESA ECONÔMICA, Conselho Administrativo et al. Prevenção e detecção de Cartéis em Licitações. 2019. Disponível em [https://repositorio.enap.gov.br/bitstream/1/6495/3/Mod%203\\_Repress%c3%a3o%20a%20Cart%c3%a9is.pdf](https://repositorio.enap.gov.br/bitstream/1/6495/3/Mod%203_Repress%c3%a3o%20a%20Cart%c3%a9is.pdf). Acesso em: 25 de out. de 2023

<sup>26</sup> Dados obtidos em pedido de acesso à informação realizado por meio da Fala.br respondido pelo órgão implementador no dia 19 de outubro de 2023.

aplicada a ferramenta demanda que o acesso a ela seja restrito (art. 23, Inc. VIII da Lei 12.527/2011)<sup>27</sup>.

### **Sinesp Big Data**

Segundo a Diretoria de Inteligência Penitenciária do MSJP, o Sinesp Big Data pode ser compreendido como a composição da soma dos entregáveis do projeto referentes à Plataforma Big Data. Este produto é um conjunto de sistemas harmonicamente integrados, composto por um orquestrador de micros serviços, sistemas de bancos de dados relacionais e não relacionais e sistemas de observabilidade - logs e monitoramento de métricas. O objetivo da plataforma é promover o desenvolvimento de uma plataforma inovadora, que permitirá integrar e analisar fontes de dados de interesse para a segurança pública, possibilitando a consolidação de um novo modelo de governança das estratégias de segurança pública, para descoberta de padrões, detecção de anomalias e predição de crimes.<sup>28</sup>

A ferramenta apresenta como público-alvo os gestores e servidores públicos em âmbito nacional, com exceção do Sinesp Cidadão que é um aplicativo mobile disponibilizado ao público. Ainda, é uma ferramenta desenvolvida no setor público. Segundo o órgão implementador, o Sinesp Big Data foi desenvolvido por meio de Termo de Execução Descentralizada entre a SENASP e a Universidade Federal do Ceará - UFC.<sup>29</sup> Cabe mencionar que a ferramenta atua em análises estatísticas, preditivas, prescritivas, diagnósticas e detecção de eventos complexos. O órgão, contudo, não especificou em quais contextos são feitas tais análises.

### **Sistema Alerta Brasil**

O Sistema Alerta Brasil foi desenvolvido pela PRF e tornou-se a principal ferramenta de monitoramento de tráfego em rodovias federais utilizadas pelo órgão a partir de 2013. Desde então, as equipes de tecnologia vêm aprimorando as técnicas

---

<sup>27</sup> Informação obtida por meio de pedido de acesso à informação na plataforma Fala.br respondido pelo órgão implementador no dia 19 de outubro de 2023.

<sup>28</sup> Dados obtidos em pedido de acesso à informação realizado por meio da Fala.br respondido pelo órgão implementador no dia 9 de outubro de 2023.

<sup>29</sup> Dados obtidos por meio de pedido de acesso à informação na plataforma Fala.br respondido pelo órgão implementador no dia 9 de outubro de 2023.

de inteligência artificial, ampliando os pontos de captura de imagens e sua capacidade de “leitura” e cruzamento de dados referentes às centenas de veículos que circulam nas rodovias federais do país. Tais técnicas de monitoramento de veículos nas rodovias federais por meio de câmeras com leitor de placas utilizam algoritmos de análise para gerar indicativos de abordagem policial. Segundo informações contidas em relatórios da PRF, no último ano, houve um acréscimo de 175% nos pontos de monitoramento em todo o país<sup>30</sup>.

Quanto às categorias de aplicação do sistema, é possível observar a classificação de imagens para reconhecimento ótico de caracteres, com foco em placas de veículos<sup>31</sup>. As variáveis de entrada são textos e imagens, já as variáveis de saída consistem em alertas enviados à central de comando e controle<sup>32</sup>. Trata-se de uma ferramenta que tem como público-alvo a gestão pública interna, e apoia o processo de decisão ao fazer diagnósticos apesar de não sugerir ações. Segundo o órgão, o Sistema Alerta Brasil foi desenvolvido por servidores da PRF, mas a solução de coleta e entrega de dados é contratada, sendo a atual fornecedora a empresa Sinalização de Trânsito Industrial Ltda (SITRAN)<sup>33</sup>.

Segundo a PRF, a ferramenta oferece subsídios para o processo de decisão por meio de alertas de passagem de veículos com registro de roubo/furto, mas não faz diagnósticos nem toma decisões sem supervisão humana, e não sugere ações<sup>34</sup>. Em 2022, o Alerta Brasil foi integrado ao Sistema Córtex, o qual dispõe de acesso a mais bases de dados pessoais, e que será apresentado a seguir.

## Sistema Córtex

---

<sup>30</sup> Informações disponíveis em: <https://portal.connectedsmartcities.com.br/2021/08/10/tecnologia-de-monitoramento-em-rodovias-reforca-acoes-da-prf-em-todo-o-brasil/>. Acesso em 26 de outubro de 2023.

<sup>31</sup> Dados obtidos por meio de pedido de acesso à informação Fala.br respondido pelo órgão implementador no dia 16 de novembro de 2023.

<sup>32</sup> Dado obtido por meio de um *powerpoint* disponibilizado pelo MJSP. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cspcco/apresentacoes-em-eventos/eventos-em-2019/EduardoMunizPolicialRodovirioFederal.pdf>. Acesso em 26 de outubro de 2023.

<sup>33</sup> Dados obtidos por meio de pedido de acesso à informação Fala.br respondido pelo órgão implementador no dia 16 de novembro de 2023.

<sup>34</sup> Dados obtidos por meio de pedido de acesso à informação Fala.br respondido pelo órgão implementador no dia 16 de novembro de 2023.

O CórteX é um sistema de informações que realiza consultas em bases de dados com acesso a sigilosas e sensíveis de cidadãos e empresas como a Relação Anual de Informações Sociais (Rais), do Ministério da Economia. Por meio da ferramenta, os oficiais credenciados podem ter acesso a dados cadastrais e trabalhistas que todas as empresas têm sobre seus funcionários, incluindo RG, CPF, endereço, dependentes, salário e cargo.<sup>35</sup> A ferramenta atua no monitoramento de alvos de interesse de segurança pública e no recebimento de alertas de alvos móveis com indicativo de criminalidade por sensores que possuem a tecnologia capaz de enviar tais informações.<sup>36</sup>

O sistema é regulamentado pela Portaria nº 218, de 21 de setembro de 2021<sup>37</sup>, a qual dispõe sobre a Plataforma Integrada e Monitoramento de Segurança Pública - CórteX. O artigo 2º da portaria aponta os objetivos do sistema

Art. 2º O CórteX é um sistema de informação que tem como objetivos:

I - a gestão de operações de segurança pública para a atuação integrada entre os órgãos do Sistema Único de Segurança Pública - Susp e instituições colaboradoras;

II - o monitoramento de atividades e indicadores oriundos da execução das operações de segurança pública; e

III - o provimento de consciência situacional por meio de funcionalidades desenvolvidas a partir da integração a webservices de interesse da segurança pública. (BRASIL, 2021a, p. 1)

Segundo a Secretaria Nacional de Segurança Pública do MJSP, a ferramenta foi desenvolvida internamente, atendendo requisitos e regras de negócio definidas por profissionais de segurança pública, com o intuito de fornecer ao profissional de segurança pública fontes de consultas e alertas de interesse visando o aprimoramento do serviço policial e redução da criminalidade. Em relação ao modelo estatístico utilizado na ferramenta, o órgão implementador afirma que, até o momento de realização desta pesquisa, não se vislumbra um modelo estatístico sedimentado, a geração de alerta é dada por uma condição específica. (Ex.: Interação de um procurado da justiça com dispositivo integrado ao córtex gera um alerta). Os *outputs* se referem às soluções buscadas em bases de dados consumidas pelo CórteX. A

<sup>35</sup> Informação disponível em <https://www.intercept.com.br/2020/09/21/governo-vigilancia-cortex/>. Acesso em 24 de outubro de 2023.

<sup>36</sup> Dados obtidos em pedido de acesso à informação realizado por meio da Fala.br respondido pelo órgão implementador no dia 2 de outubro de 2023.

<sup>37</sup> Disponível em <https://www.gov.br/mj/pt-br/assuntos/sua-seguranca/seguranca-publica/operacoes-integradas/cortex/publicacoes/portaria-no-218-de-29-de-setembro-de-2021/view>. Acesso em 26 de outubro de 2023.

ferramenta consome bases de diversas fontes e organiza resultados, seja para consulta, seja para geração de alertas.<sup>38</sup>

A respeito do seu grau de apoio no processo de decisão oferecido pela ferramenta, o órgão informou que o Córtex faz diagnósticos, mas não sugere ações. Segundo o órgão, a ferramenta gera alertas, seja através de uma consulta (ex: ao consultar uma placa, avisa que o veículo é roubado), ou mesmo de forma automática (ex: avisa que determinado veículo roubado acabou de passar em determinado logradouro). Para mais, os diagnósticos feitos pela ferramenta são realizados de acordo com a consulta em diversas bases de dados integradas ao córtex. Caso o alerta/resultados da consulta esteja incorreto, o órgão informa que se trata de problema na fonte de leitura de dados e não no sistema. Todavia, casos de erro são relatados pelos usuários para verificação na fonte de dados.<sup>39</sup>

### **Solução Automatizada de Identificação Biométrica (ABIS)**

ABIS refere-se a uma categoria de Sistemas Automatizados de Identificação Biométrica (Automated Biometric Identification Systems). Segundo informações oferecidas pela Polícia Federal, a ferramenta é aplicada para a comparação de imagens biométricas<sup>40</sup>. Ainda, o órgão informou que o objetivo da ABIS é de prover à Polícia Federal e órgãos congêneres o armazenamento e processamento de informações biométricas. Trata-se, desse modo, de uma ferramenta que pode ser utilizada para reconhecimento biométrico facial, não sendo especificado pelo órgão qual é sua categoria de aplicação. A ABIS é desenvolvida para acomodar dados de 50,2 milhões de pessoas ao longo de 48 meses, com a capacidade de expansão futura para incluir dados de até 200 milhões de indivíduos<sup>41</sup>.

---

<sup>38</sup> Dados obtidos em pedido de acesso à informação realizado por meio da Fala.br respondido pelo órgão implementador no dia 2 de outubro de 2023.

<sup>39</sup> Dados obtidos em pedido de acesso à informação realizado por meio da Fala.br respondido pelo órgão implementador no dia 2 de outubro de 2023.

<sup>40</sup> Dados obtidos em pedido de acesso à informação realizado por meio da Fala.br respondido pelo órgão implementador no dia 18 de outubro de 2023.

<sup>41</sup> Dados obtidos em : <https://www.gov.br/pf/pt-br/assuntos/noticias/2021/07/policia-federal-implementa-nova-solucao-automatizada-de-identificacao-biometrica>. Acesso em 20 de novembro de 2023.

Não se trata de uma ferramenta desenvolvida no setor público, a PF informa que, após o Pregão Eletrônico nº 4/2020 - DTI/PF<sup>42</sup>, foi selecionada uma fornecedora para adaptar seu produto ABIS de acordo com as especificações da Polícia Federal. O órgão, contudo, não apresentou especificações acerca da empresa fornecedora. Ainda, a PF informou que não obteve informações acerca do modelo estatístico utilizado na ferramenta, e que os mecanismos de codificação e de comparação biométricas da ferramenta seguem o modelo do proprietário desenvolvedor, podendo conter diferentes modelos estatísticos aplicados.<sup>43</sup>

Por se tratar de uma ferramenta adquirida no setor privado, a PF informou que não detém conhecimento acerca dos conjuntos de variáveis usados como entrada para treinamento para a ferramenta, e que os dados da PF não foram utilizados no desenvolvimento da ABIS. Assim como a Databricks, caso tenha sido comprada pronta de empresa estrangeira, esta ferramenta relaciona-se com as ideias de Morozov (2018), as quais indicam que países como o Brasil, são dependentes das tecnologias de países com soberania tecnológica. Neste caso, a situação é especialmente alarmante pois não há acesso por parte da administração pública brasileira às bases de dados utilizadas pelos desenvolvedores da ferramenta, nem se os dados armazenados pela ferramenta serão compartilhados com os servidores da empresa fornecedora da ferramenta.

Em relação às saídas da ferramenta, a PF aponta para uma lista dos candidatos, ordenada da maior convergência para a menor, onde exista um grau de convergência com a imagem biométrica. Em alguns casos, a saída é a informação de convergência ou não das biometrias<sup>44</sup>.

### **Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa**

---

<sup>42</sup> Informações disponíveis acerca do Pregão eletrônico em: <https://www.gov.br/pf/pt-br/assuntos/licitacoes/2020/distrito-federal/orgaos-centrais/dti/pregoes/pregao-eletronico-ndeg-4-2020-dti-pf>. Acesso em: 26 de out. de 2023.

<sup>43</sup> Dados obtidos em pedido de acesso à informação realizado por meio da Fala.br respondido pelo órgão implementador no dia 18 de outubro de 2023.

<sup>44</sup> Dados obtidos em pedido de acesso à informação realizado por meio da Fala.br respondido pelo órgão implementador no dia 18 de outubro de 2023.

Esta ferramenta foi mapeada por meio do algoritmo de busca automatizada, e todos os dados obtidos a seu respeito encontram-se no *Catálogo de Uso de Inteligência Artificial por Órgãos Governamentais* elaborado e disponibilizado pela Transparência Brasil. Um dos principais objetivos dessa Organização da Sociedade Civil (OSC) é oferecer instrumentos de monitoramento de instituições públicas para a sociedade, e um dos seus projetos, o *Transparência Algorítmica*, foca no monitoramento das iniciativas de IA utilizadas pelo governo. Com isso, tal organização indicou a Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa como uma das ferramentas de IA utilizadas pela Comissão de Valores Imobiliários (CVM). A CVM, todavia, ao ser questionada sobre tal ferramenta, afirmou que não dispõe de iniciativas baseadas em IA. Optou-se por analisar a ferramenta e adotá-la como objeto de estudo desta pesquisa, tendo em vista que esse configura mais um caso de opacidade algorítmica e opacidade da gestão, assim como ocorreu com a A.I Desk e com o PalasNet.

Ferramenta implementada pela Comissão de Valores Mobiliários (CVM), a solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa refere-se a um algoritmo que auxilia na supervisão de possíveis ilícitos no mercado de capitais. É uma solução voltada para a gestão pública interna, e sua categoria de aplicação consiste em estimativas de risco, incluindo detecção de fraudes na bolsa de valores. O modelo estatístico empregado na ferramenta é o de regras de negócio/heurísticas e probabilidade Bayesiana.<sup>45</sup>

Acerca das variáveis de entrada da ferramenta, a CVM informa que, pela natureza da ferramenta, a divulgação das variáveis poderia comprometer os resultados. Todavia, o órgão pôde citar algumas das variáveis: idade do investidor, tempo de atuação do investidor no mercado, histórico de atuação do investidor. Já suas saídas consistem nas listas de transações suspeitas de práticas ilegais em negociações no mercado da bolsa de valores. Desse modo, a ferramenta faz diagnósticos, mas não sugere ações.<sup>46</sup>

---

<sup>45</sup> Dados obtidos em: “Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de de bolsa.” *Catálogo de Uso de Inteligência Artificial por Órgãos Governamentais*, acesso em 27 de outubro de 2023, <https://catalogoia.omeka.net/items/show/27>.

<sup>46</sup> Dados obtidos em: “Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de de bolsa.” *Catálogo de Uso de Inteligência Artificial por*

A ferramenta foi desenvolvida pela equipe interna em parceria com uma empresa terceirizada. Não foram encontrados dados, porém, acerca da empresa contratada. Em relação a seu efeito no processo decisório, a ferramenta realiza diagnósticos, mas não sugere ações. Dessa forma, cabe aos servidores da área responsável pela atividade de supervisão e sanção do órgão receberem as indicações de transações suspeitas da ferramenta e avançarem com o trabalho humano de investigação.<sup>47</sup>

#### 4.2 Iniciativa da Sociedade Civil em Parceria com o Governo Federal

O intuito inicial da pesquisa era mapear apenas as iniciativas implementadas pelo governo federal. Contudo, no processo de coleta de dados para realização da pesquisa, foi encontrada uma iniciativa voltada para segurança pública de uma Organização da Sociedade Civil, o Instituto Glória, idealizada por Cristina Castro, professora e pesquisadora do Instituto de Ciências Biológicas da Universidade de Brasília. Ao levar em consideração que a ferramenta pode ter contato direto com cidadãos brasileiros, e que um dos objetivos da ferramenta consiste na coleta de dados para a melhoria das políticas públicas, optou-se por tratar tal ferramenta como objeto de análise. A seguir, será apresentada tal ferramenta, o Robô Glória.

#### Robô Glória

Fruto do Projeto Glória, o Robô Glória é uma interface de comunicação com mulheres e meninas vítimas de violência, focada no apoio e na busca de soluções para cada caso. Não se trata de um *chatbot* com respostas prontas, tendo em vista que a ferramenta reúne um conjunto de algoritmos com capacidade de aprendizado. Assim, o robô virtual evolui por meio de interações em linguagem natural com os usuários. Segundo informações divulgadas pela *website* do Instituto Glória<sup>48</sup>, a Glória

---

Órgãos Governamentais, acesso em 27 de outubro de 2023, <https://catalogoia.omeka.net/items/show/27>.

<sup>47</sup> Dados obtidos em: "Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de de bolsa.," *Catálogo de Uso de Inteligência Artificial por Órgãos Governamentais*, acesso em 27 de outubro de 2023, <https://catalogoia.omeka.net/items/show/27>.

<sup>48</sup> Disponível em <https://www.eusouagloria.com.br/>. Acesso em: 28 de out. de 2023.

é baseada em três pilares: *machine learning*, *people analytics* (gestão de pessoas baseado em dados) e *skills management* (habilidades de gestão).

O Projeto Glória nasceu a partir do dado que indica o sentimento de vergonha como um dos principais obstáculos que impede as mulheres em situação de violência doméstica de denunciar o agressor. Nesse sentido, o robô virtual, por ser capaz de acumular conhecimentos e aprender sobre os comportamentos a cada interação, oferece alternativas às vítimas, como incentivo à denúncia e apoio jurídico.

Além de oferecer apoio a mulheres e meninas em situação de violência, o projeto também intenta coletar dados e gerar relatórios que possam auxiliar o poder público na formação de políticas, projetos e ações para combater a violência contra a mulher. Ao entrar em contato com a plataforma inteligente, a vítima pode escolher informar dados como idade, localização, dados socioeconômicos, mas sem necessidade de se auto identificar. Com isso, o projeto intenta minerar dados exatos e gerar mapas com mais informações sobre o perfil de quem sofre violência.<sup>49</sup>

Com base no exposto, observa-se que a ferramenta é voltada para dois públicos-alvo externos ao Instituto Glória, as cidadãs e a gestão pública. Em relação ao seu grau de apoio no processo decisório de cada público, o robô faz diagnósticos e sugere ações para as cidadãs, e faz diagnósticos e mas não sugere ações para gestão pública. Cabe ressaltar que os diagnósticos levantados pelo robô contam com revisão humana.

O Projeto Glória é uma iniciativa sem fins lucrativos, que conta com voluntários em todo o Brasil entre programadores, advogados e psicólogos. No Distrito Federal, local de origem do projeto, a ferramenta tem apoio de entidades como o Instituto Federal de Brasília (IFB) e a Universidade de Brasília (UnB). Além disso, empresas globais como Google e Microsoft também fornecem suporte ao projeto.

### **4.3 Uso de ferramentas de IA e aumento de eficiência na gestão pública**

Conforme abordado no capítulo do Referencial Teórico, eficiência é um dos princípios que regem a Administração Pública Brasileira, e envolve questões como a

---

<sup>49</sup> Dados obtidos em <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/comissao-de-defesa-dos-direitos-da-mulher-cmulher/noticias/lancamento-do-projeto-gloria>. Acesso em 28 de out. de 2023.

otimização da utilização de recursos públicos e a busca pela qualidade dos bens e serviços ofertados aos cidadãos (DI PIETRO, 2005; MORAIS, 2009). Desse modo, para garantir a eficiência na gestão pública, é indispensável a busca por métodos na gestão de recursos públicos que proporcionem o atendimento às demandas sociais, de modo a garantir a efetividade de direitos fundamentais e fortalecer, assim, a democracia (DAHL, 1998; DESORDI & BONA, 2020).

Tendo em vista o grande crescimento das responsabilidades estatais nas últimas décadas, o aumento dos deveres da gestão pública culminou em alguns desafios, como déficit de pessoal, obstáculos burocráticos e restrições orçamentárias (DESORDI & BONA, 2020). Segundo Desordi e Bona (2020), tais gargalos geram insatisfação interna e externa pela carência na prestação do serviço público, e o agente público carece de instrumentos inovadores para alcançar a eficiência administrativa almejada. Segundo Fountain (2001), as inovações tecnológicas, como as baseadas em Inteligência Artificial (ARAÚJO, ZULLO E TORRES, 2020), criam oportunidades para remodelar a gestão pública e promover ganhos de eficiência que a permitam melhorar sua oferta de serviços, ao viabilizar a automatização e simplificação de processos administrativos e/ou operacionais.

Ademais, o uso de tais tecnologias é recorrentemente voltado para identificação de transações fraudulentas, seja fraudes cometidas por cidadãos ou ao combater a corrupção por parte dos agentes públicos (ARAÚJO, ZULLO E TORRES, 2020). Tendo em vista que a corrupção e a ocorrência de fraudes no âmbito público podem representar um entrave para a eficiência na gestão pública conforme indicam Toyoshima & Lopes (2013), ferramentas com capacidade de detectar transações fraudulentas, seja fraudes cometidas por cidadãos ou para combater a corrupção por parte dos agentes públicos, apresentam grande importância para assegurar que a máquina pública possa contar com a totalidade de seus recursos para a garantia do bem-estar social. Assim, tais mecanismos tecnológicos criam oportunidades para possibilitar a manutenção de um ambiente democrático, uma vez que, na atual crise das democracias liberais, a corrupção é um fator que enfraquece a confiança dos cidadãos nos Estados (CASTELLS, 2018).

Nesse entendimento, pretende-se observar como as ferramentas de IA voltadas para a área de Segurança Pública mapeadas neste estudo podem contribuir para o aumento da eficiência na gestão pública brasileira, observando alguns critérios baseados no Referencial Teórico deste trabalho. No primeiro momento, são

abordados os dados referentes ao desempenho e/ou resultados alcançados pelos órgãos públicos em relação às iniciativas que utilizam recursos de IA na área de segurança pública por meio de pesquisa bibliográfica e pesquisa documental.

No segundo momento, pretende-se aferir, a partir do ponto de vista dos órgãos implementadores, se as ferramentas já utilizadas:

- A. promoveram melhorias em processos administrativos e/ou operacionais; e
- B. permitem que os agentes públicos desempenhem melhor a sua rotina e, assim, sejam capazes de entregar bens e serviços com mais qualidade aos cidadãos.

Tais informações foram obtidas por meio de solicitações de acesso à informação realizadas na plataforma Fala.br que foram respondidas pelos órgãos implementadores.

#### **4.3.1 Apresentação do desempenho e/ou dos resultados alcançados pelas ferramentas baseadas em IA utilizadas na Gestão Pública**

Dentre as ferramentas desenvolvidas dentro da Perícia da Polícia Federal é possível destacar o Localizador de Evidências Digitais (LED), o Nudetective e o A.I Desk. Essas três ferramentas compartilham um propósito comum: auxiliar o policial em operações de busca e apreensão de dispositivos de informática associados à pornografia infantojuvenil, agilizando a identificação e classificação, de maneira rápida e eficaz, dos vestígios de interesse para uma intervenção rápida e eficaz.

Quanto ao desempenho do A.I Desk, a análise realizada no artigo *A Benchmark Methodology for Child Pornography Detection*, escrito pelos desenvolvedores da ferramenta, demonstra que o sistema A.I Desk registrou 79.84% de acurácia nas imagens analisadas, e que os casos em que sua eficácia é comprometida são provenientes de quando se trata de imagens pornográficas infantis sem rostos de crianças. Dessa forma, os autores indicaram que o instrumento possui uma taxa de sucesso satisfatória, mas que ainda requer aprimoramentos (MACEDO & COSTA, 2018).

Na edição 42, *Infância Interrompida* da revista Perícia Federal<sup>50</sup>, o desenvolvedor do software LED, o Perito Criminal Federal Wladimir Leite, compartilha

---

<sup>50</sup> Disponível em: <https://apcf.org.br/revistas/edicao-no-42-infancia-interrompida/>. Acesso em 10 de outubro de 2023.

que o grande benefício do programa se refere, na maioria dos casos, à sua capacidade de determinar se um arquivo é suspeito sem a necessidade de varrer integralmente o seu conteúdo. O tempo despendido efetivamente para análise dos arquivos varia consideravelmente conforme o volume e as características dos arquivos identificados, mas, em linhas gerais, a análise de um disco de 500 GB é concluída em menos de 10 minutos. Ainda segundo Wladimir, uma característica crucial do software é a apresentação contínua de resultados parciais ao perito durante a varredura, permitindo que os agentes públicos possam agir mesmo antes da conclusão do processo. Por fim, na revista consta que o programa já é amplamente utilizado por parte dos peritos criminais federais da área de informática voltados para esse tipo de delito, além de algumas unidades de perícias estaduais, que tomaram conhecimento da ferramenta e a utilizam.

Já em relação à performance do NuDetective, o artigo *NuDetective: A Forensic Tool to Help Combat Child Pornography through Automatic Nudity Detection*<sup>51</sup>, elaborado pelos desenvolvedores da ferramenta, apresenta dois experimentos de avaliação da ferramenta, nos quais foram apresentadas taxas de detecção em torno de 95%, com baixas taxas de falsos positivos, aliadas à rapidez de processamento.

Em relação ao tempo de resposta na identificação de material suspeito, o Perito Criminal Federal Pedro Eleutério indica que depende do conteúdo da mídia. Ele relata que, em testes laboratoriais, foi possível processar um disco rígido com mais de 300.000 arquivos em 12 minutos. No entanto, esse tempo pode variar com base no conteúdo e na resolução das fotos. Se houver muitas fotos em alta resolução, o processo pode levar um pouco mais, pois a detecção ocorre com base no conteúdo da própria imagem. Ainda, o PCF ressalta a rapidez da ferramenta na análise de vídeos, onde, apesar de serem arquivos maiores, alguns frames são extraídos sem a necessidade de renderização ou leitura completa do arquivo de vídeo. O tempo médio gasto para analisar um arquivo de vídeo de qualquer tamanho é de aproximadamente 1 segundo.<sup>52</sup>

Além disso, no artigo *An overview of NuDetective Forensic Tool and its usage to combat child pornography in Brazil*, os autores da ferramenta Silva e Polastro

---

<sup>51</sup> Disponível em: <https://ieeexplore.ieee.org/abstract/document/5591120/references#references>. Acesso em 3 de outubro de 2023.

<sup>52</sup> Informações obtidas em <https://apcf.org.br/revistas/edicao-no-42-infancia-interrompida/>. Acesso em 10 de outubro de 2023.

(2014), realizaram uma pesquisa para avaliar a eficácia do NuDetective por seus usuários brasileiros em casos reais. Os resultados da pesquisa demonstraram que, dos 28 usuários participantes, cerca de 79% deles utilizavam a ferramenta em pelo menos um caso forense real. Além disso, 74% dos usuários que utilizaram a ferramenta em casos forenses reais encontraram arquivos de pornografia infantil em mídia digital usando a ferramenta (SILVA & POLASTRO, 2014). Dessa forma, com os resultados supracitados acerca do uso da ferramenta, os autores concluíram que a ferramenta contribui para seu objetivo principal, que é auxiliar no combate à pornografia infantil.

No âmbito das ferramentas que fazem uso de IA voltadas para videomonitoramento, implementadas pelos órgãos de Segurança Pública, é possível citar o Sistema Alerta Brasil da PRF e o Sistema Córtex do MJSP. Em 2019, ambas ferramentas se uniram para operacionalizar o maior sistema de monitoramento viário do Brasil, o Alerta Brasil 3.0. Segundo a Associação Brasileira de Transporte e Logística de Produtos Perigosos (ABTLP), o intuito da fusão é fomentar cada vez mais a integração entre os órgãos de segurança, visando aprimorar as ações voltadas para o enfrentamento da criminalidade e garantir a segurança viária nas rodovias federais em todo o território nacional. Além disso, a associação aponta que integrar os sistemas significa ampliar a rede de proteção e monitoramento, resultando em maior capacidade de geração e armazenamento de dados a um baixo custo operacional, benefício proporcionado pela tecnologia do Córtex. Contudo, tal processo vai além da otimização de recursos financeiros e materiais; o Alerta Brasil 3.0 influencia diretamente o recurso humano. Os órgãos de segurança passaram a compor uma rede de compartilhamento de informações, que servirá de base para planejamentos operacionais e orientação dos trabalhos de inteligência policial.<sup>53</sup>

Segundo a apresentação da PRF disponibilizada pelo Portal da Câmara dos Deputados<sup>54</sup>, o Sistema Alerta Brasil, lançado em 2013, obteve alguns resultados operacionais alcançados. Dentre esses resultados, é possível citar o aumento em 600% de apreensões de drogas pela PRF em 2019. Neste ano, a PRF apreendeu

---

<sup>53</sup> Informações obtidas em <https://www.abtlp.org.br/index.php/tecnologias-da-prf-seopi-e-senasp-sao-integradas-para-operacionalizar-o-maior-sistema-de-monitoramento-viario-do-pais/>. Acesso em 30 de outubro de 2023.

<sup>54</sup> Informações obtidas por meio de pdf elaborado pela PRF. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cspcco/apresentacoes-em-eventos/eventos-em-2019/EduardoMunizPolicialRodovirioFederal.pdf>. Acesso em: 30 de outubro de 2023.

cerca de 8,6 milhões de pacotes de cigarros e sete toneladas de agrotóxico contrabandeados; 10,9 mil metros de madeira ilegal; 247 toneladas de maconha; outras 16 toneladas de cocaína; 1,2 mil armas de fogo e 56 mil munições; e recuperou mais de 4,6 mil veículos com registro de roubo ou furto<sup>55</sup>. Ademais, o órgão foi capaz de melhorar índices no Ceará a partir da implementação do sistema. Em 2017, o Ceará chegava à marca de 5 mil assassinatos, além da média de 24 carros roubados por dia. A partir da implementação do Sistema Alerta Brasil 3.0, o Ceará se tornou o estado que mais reduziu homicídios de janeiro a maio, e os roubos de veículos no estado reduziram 48% no primeiro semestre de 2019<sup>56</sup>. É importante ressaltar que o órgão tem interesse em divulgar bons resultados advindos do uso da ferramenta, mesmo que a redução de índices de criminalidade e o aumento da apreensão de drogas não apresentem ligação direta com o uso da ferramenta.

Foi possível coletar resultados de ferramentas voltadas para combate a corrupção e fraudes no setor público, do Projeto Cérebro e do Delphos. Tais ferramentas são particularmente importantes para a gestão pública, tendo em vista que a corrupção é um dos fatores responsáveis pela queda dos regimes democráticos liberais no mundo (CASTELLS, 2018), bem como por reduzir as capacidades estatais da administração pública e impactar negativamente sua eficiência (TOYOSHIMA & LOPES, 2013).

O Projeto Cérebro apresenta técnicas algorítmicas de análise de dados baseadas em licitações públicas para permitir a identificação de indícios de atuação coordenada em compras públicas. Em relação à existência de evidências empíricas em que o algoritmo da ferramenta funcione no ambiente em que ele está sendo utilizado, De Defesa Econômica (2019) aponta para a importância do projeto na Operação Mercador de Veneza e na Operação Porto de Encontro. Na primeira, investigou cartéis em licitações relacionadas à aquisição de órteses, próteses e materiais especiais. Nessa operação, a ferramenta atuou na identificação de alvos prioritários com mais elevado número de indícios para a diligência de busca e apreensão. Essa estratégia permitiu uma abordagem mais eficiente e direcionada na

---

<sup>55</sup> Dados obtidos em <https://www.abtbp.org.br/index.php/tecnologias-da-prf-seopi-e-senasp-sao-integradas-para-operacionalizar-o-maior-sistema-de-monitoramento-viario-do-pais/>. Acesso em 26 de outubro de 2023.

<sup>56</sup> Informações obtidas por meio de pdf elaborado pela PRF. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cspcco/apresentacoes-em-eventos/eventos-em-2019/EduardoMunizPolicialRodovirioFederal.pdf>. Acesso em: 30 de outubro de 2023.

investigação de possíveis práticas cartelizadas nesse setor. Já na segunda operação, a ferramenta investigou as empresas envolvidas em licitações para a contratação de serviços terceirizados. Com o auxílio do Cérebro, foi possível identificar as empresas que se tornaram alvo das operações de busca e apreensão.

Acerca do Delphos, há um artigo disponibilizado em meio de comunicação online<sup>57</sup> redigido pelo presidente da Associação Nacional dos Peritos Criminais Federais (APCF), no qual são elucidadas algumas informações acerca do uso desta ferramenta, em especial no caso de investigação das suspeitas de corrupção em gastos públicos relacionados à pandemia do novo coronavírus. No artigo, o perito informa que o sistema é alimentado com informações das contratações feitas por entes públicos de todo o país e, a partir disso, há o cruzamento do conteúdo de outros bancos de dados. A ferramenta atuou para resolver o problema da falta de padronização da grande quantidade de informações prestadas pelos governos municipais, estaduais e federal sobre as contratações motivadas pela Covid-19. Nesse sentido, o perito afirma que o sistema permite que os peritos criminais federais localizem evidências da ocorrência de sobrepreço e de superfaturamento nas contratações de forma mais ágil, além de levantar indícios acerca das irregularidades nas empresas contratadas.

Tais ferramentas, se implementadas com devida regulamentação jurídica, apresentam alto potencial para gerar benefícios para toda a administração pública e para a população em geral. Como a corrupção é um fator que limita as capacidades estatais e reduz a eficiência na gestão pública (TOYOSHIMA & LOPES, 2013), tais ferramentas não só podem apoiar atividades dos órgãos que as implementam, mas também contribuir para recuperação de recursos públicos que poderiam ser alocados em outros órgãos.

Cabe ressaltar que todos os resultados aqui analisados foram colhidos pelos próprios órgãos implementadores das iniciativas que utilizam recursos de IA, ou pelos seus desenvolvedores. Isso pode justificar a somente disponibilização de resultados positivos das ferramentas, tendo em vista que é de interesse dos órgãos desenvolvedores/implementadores o enaltecimento e sucesso de suas ferramentas. O interessante seria que houvesse pesquisas feitas pelo Ministério Público Federal

---

<sup>57</sup> Artigo disponível em <https://www.gazetadopovo.com.br/opiniao/artigos/delphos-a-contribuicao-da-pericia-criminal-da-pf-contra-a-corrupcao-na-pandemia/>. Acesso em: 18 de out. 2023.

(MPF) ou pelo Tribunal de Contas da União (TCU), ou mesmo por outros membros da sociedade civil, que indicassem os resultados dos órgãos a partir do uso das ferramentas. Contudo, não foi possível encontrar nenhuma avaliação dessas organizações acerca das ferramentas.

Não foi possível encontrar informação pública suficiente para conduzir a apresentação dos resultados e performances referentes às ferramentas D.E.I.A. - Defesa Econômica com Inteligência Artificial, DataBricks, PalasNET, Sinesp Big Data, Solução Automatizada de Identificação Biométrica (ABIS) e a Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa. Isso pode ser justificado pela recenticidade de aplicação das ferramentas, sendo que grande parte da implementação delas teve início em 2022 e em 2023, como é o caso D.E.I.A. - Defesa Econômica com Inteligência Artificial e da Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa.

Já acerca do DataBricks e da Solução Automatizada de Identificação Biométrica (ABIS) compradas em 2020 pelos órgãos implementadores, não foi possível encontrar, por meio eletrônico, informações suficientes acerca de seus resultados, nem de sua performance. Por fim, não foi possível obter informações profundas sobre os resultados alcançados pelo Robô Glória para a gestão pública no que diz respeito aos relatórios que poderiam auxiliar o poder público na formação de políticas, projetos e ações para combater a violência contra a mulher. A única informação encontrada em meio eletrônico sobre os resultados do Robô Glória refere-se ao dado de que, desde o lançamento do projeto em 2019, mais de dois milhões de pessoas usaram a Glória<sup>58</sup>

#### **4.3.2 Análise da eficiência das ferramentas de IA com base na visão do órgão implementador/desenvolvedor**

A partir de pedidos de acesso à informação enviados aos órgãos do governo federal desenvolvedores e/ou implementadores das treze (13) ferramentas de IA orientadas para área de Segurança Pública mapeadas por este estudo, foram obtidas

---

<sup>58</sup> Informação disponível em <https://www.correiobraziliense.com.br/euestudante/ensino-superior/2023/07/5108621-robo-brasiliense-contr-a-violencia-de-genero-chega-a-190-paises.html>. Acesso em 20 de outubro de 2023.

dez (10) respostas relativas à capacidade das tecnologias de viabilizar melhorias em processos administrativos e/ou operacionais. Ainda, como abordado no capítulo da Metodologia, foi enviado um questionário ao Instituto Glória com o propósito de verificar quais objetivos o Robô Glória alcançou, bem como se os relatórios que a ferramenta pretendia gerar para delinear o perfil de quem sofre violência foram efetivamente utilizados pela gestão pública. O Instituto, porém, não retornou resposta acerca disso.

Dentre as dez respostas recebidas, a ABIS ainda se encontra em processo de início de implementação e, por isso, a Polícia Federal atestou que ainda não foi possível verificar se tal tecnologia possibilitou melhorias em processos administrativos e/ou operacionais, nem se foi capaz de permitir que os agentes públicos desempenhem melhor a sua rotina.

Em relação às outras dez ferramentas já implementadas sobre as quais foi possível obter as respostas dos órgãos, pode-se citar a D.E.I.A., a DataBricks, o Delphos, o LED, o NuDetective, PalasNET, o Projeto Cérebro, o Sistema Alerta Brasil, o Sistema Córtex e a Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa.

Na Tabela 2 é exposto, a partir do ponto de vista dos órgãos, se as ferramentas foram capazes de promover melhorias em processos administrativos e/ou operacionais (Ponto A) e de permitir que os agentes públicos desempenhem melhor a sua rotina e sejam capazes de entregar bens e serviços com mais qualidade aos cidadãos (Ponto B).

**Tabela 2** - Capacidade da ferramenta de IA de promover eficiência a partir da perspectiva dos órgãos implementadores e/ou desenvolvedores

Ferramenta	Ponto A	Ponto B
D.E.I.A. - Defesa Econômica com Inteligência Artificial.	Sim. Tendo em vista que a ferramenta automatiza processos que anteriormente eram realizados de forma manual, a ferramenta permite o aprimoramento dos processos internos.	O uso da ferramenta permitiu que os servidores pudessem focar em outras tarefas mais complexas. Além disso, permitiu uma melhor entrega de serviços ao cidadão, pois facilita a recuperação de informações relevantes para o cidadão.
DataBricks	Sim, em termos de disponibilização de	Sim. De forma indireta foi possível identificar melhorias

	<p>dados a ferramenta permitiu acesso aos dados de forma a ser consumido para criação de painéis de BI ou mesmo para consumo de API's. A ferramenta permitiu aprimoramento nos processos internos em questão de tempo e economia de recursos, em termos de criação de painel de BI e acesso a dados via API que antes necessitavam de interação humana, bem como automatização do processo de atualização desses dados.</p>	<p>em processos, o que possibilitou ajustes para entrega de serviços com qualidade ao cidadão.</p>
Delphos	<p>Sim. O Delphos permitiu a alteração de fluxos de processos em setores das criminalísticas, orientando e automatizando tarefas relacionadas a atividades periciais.</p>	<p>Sim. Alguns dos módulos presentes na ferramenta otimizam atividades de busca de informação, com economia de tempo do servidor, além de identificar necessidades que o perito possui para tarefas rotineiras.</p>
Localizador de Evidências Digitais	<p>Sim. A ferramenta permitiu a otimização de procedimentos operacionais de cumprimento de mandados de busca e apreensão em crimes envolvendo a exploração de menores. Os alertas gerados pelo LED aumentam a chance de localização de alguns vestígios que poderiam ser difíceis de encontrar "manualmente", melhorando a qualidade do procedimento. Com isso, a ferramenta apresentou impacto positivo na produtividade do órgão.</p>	<p>A ferramenta agiliza a análise superficial realizada nos locais de busca, reduzindo o tempo de permanência da equipe policial no local e, conseqüentemente, o risco inerente a esse tipo de atividade.</p>
NuDetective	<p>Sim. A ferramenta facilita e acelera a triagem que antes era feita manualmente por meio da inspeção direta dos arquivos encontrados no computador ou celular do suspeito.</p>	<p>A ferramenta acelera a análise preliminar realizada em locais de busca, reduzindo o tempo que a equipe policial precisa permanecer no local, permitindo a prisão de suspeitos.</p>
PalasNET	<p>Sim. Com a possibilidade de consultas rápidas às informações armazenadas no banco de dados, as respostas aos processos se tornaram mais céleres, diminuindo o tempo em que o processo permanece no setor e contribui positivamente para produtividade do órgão.</p>	<p>Sim, o uso da ferramenta permitiu que os servidores pudessem focar em outras tarefas mais complexas.</p>
Projeto Cérebro	<p>Sim. Por meio da disponibilização de dados e informações focadas em</p>	<p>Sim, foi observado impacto na melhora da prestação do serviço público.</p>

	<p>auxiliar o processo de tomada de decisão nas investigações conduzidas pelo Cade, a ferramenta promove ganhos de eficiência. Neste sentido o ganho de eficiência pode aumentar, por exemplo, a capacidade de processamento de eventuais denúncias de infrações à ordem econômica.</p>	
<p>Sistema Alerta Brasil</p>	<p>Não existe estudo sobre o impacto da ferramenta nos processos internos. Porém, o Sistema Alerta Brasil faz parte da estratégia institucional de policiamento orientado à inteligência. Os resultados operacionais decorrentes do policiamento orientado à inteligência são, em parte, proporcionados pelo Alerta Brasil.</p>	<p>A ferramenta está vinculada ao cumprimento dos objetivos institucionais do órgão. Não obstante a inexistência de estudos que comprovem esta hipótese, é possível concluir que a ferramenta contribui nas entregas para a sociedade, uma vez que contribui fortemente para o enfrentamento às organizações criminosas e para a segurança viária.</p>
<p>Sistema CórTEX</p>	<p>Sim, pois a ferramenta permite a reunião de diversas bases de dados em um único local, algo que anteriormente estava disperso em vários sistemas de diferentes órgãos. A ferramenta permite o cadastro de operações, escalas de serviço e lançamento de resultados, de forma integrada, entre diversos órgãos de segurança pública, automatizando e sistematizando processos administrativos que até então eram executados de forma manual.</p>	<p>Sim, a ferramenta agiliza a sistematização de processos que antes eram executados de forma manual, promovendo economia de tempo para o servidor.</p>

Fonte: elaboração própria, 2023.

Em um panorama mais geral, com base nas respostas dos órgãos, observa-se que as ferramentas de IA empregadas estão sendo capazes de promover melhorias nos processos administrativos e/ou operacionais. Os órgãos indicam como fatores responsáveis por tais melhorias: ganhos de produtividade; automatização e sistematização de processos administrativos que antes eram realizados de maneira manual; economia de tempo e de recursos; integração de dados entre diferentes órgãos; processamento mais ágil de análise de dados; e atualização automática de dados.

Tais fatores corroboram com as ideias trazidas por Fountain (2001) acerca do uso de IA, o qual indica que tecnologias de IA podem trazer ganhos de eficiência para

os usuários ao proporcionarem a automatização de processos administrativos. Condizem, também, com o ponto de vista de Dias, Sano e Medeiros (2019), os quais apontam que a aplicação de sistemas de informação integrados e o uso de soluções tecnológicas avançadas pela gestão pública podem simplificar tarefas burocráticas, reduzindo o tempo e os recursos necessários para executá-las, além de favorecer o aumento da produtividade (DIAS, SANO & MEDEIROS, 2019).

Tais fatores também ratificam o que fora indicado por Desordi e Bona (2020), os quais demonstraram que a integração de dados entre diferentes órgãos, promovida pelo uso de sistemas de informação, resulta na melhora do fluxo de informações entre mecanismos informáticos, o que proporciona impactos positivos para a gestão. Ainda, corrobora com o que foi abordado por Campos e Figueiredo (2021), os quais demonstraram que a automatização de processos administrativos permite ampliar a capacidade de processamento e análise de dados por parte dos tomadores de decisão humanos, o que pode tornar o ciclo de políticas públicas mais eficiente.

Cabe uma ressalva em relação à resposta da PRF acerca de como o Sistema Alerta Brasil contribui para melhorias em seus processos administrativos e/ou operacionais e acerca de seus objetivos alcançados. O órgão informou que, como o sistema faz parte da estratégia institucional de Policiamento Orientado à Inteligência (POI), os resultados operacionais decorrentes do policiamento orientado à inteligência são, em parte, proporcionados pelo Alerta Brasil. Nesse sentido, a dissertação de mestrado de Brasil (2022), que procurou analisar a influência do POI no desempenho da PRF na apreensão de drogas, verificando as médias dos resultados das apreensões de drogas com e sem a participação da Inteligência. Com isso, Brasil (2022) apontou que o POI potencializa as apreensões de drogas da PRF e que as apreensões são significativamente maiores quando a Inteligência é empregada. Nesse viés, os estudos de Brasil (2022) demonstraram que, embora as ocorrências de flagrantes com a participação da Inteligência sejam menos frequentes, a média de drogas apreendidas por incidente é consideravelmente maior. Isso revelou que há uma qualidade superior nesse modelo de policiamento, tendo em vista que o POI reduz a frequência das apreensões, mas elas ocorrem em maior volume. Ao considerar que a PRF indicou que os resultados positivos do POI advêm em parte do Alerta Brasil, e que a PRF foi capaz de desempenhar melhor com o POI, é possível verificar que a solução tecnológica contribuiu para o aumento da eficiência no órgão.

A partir da análise realizada acerca da percepção dos órgãos acerca do uso das ferramentas de IA por eles desenvolvidas e/ou implementadas, foi possível perceber que as dez ferramentas analisadas estão contribuindo para o aumento da eficiência na gestão pública interna. Os dados fornecidos pelos órgãos indicam que tecnologias de IA implementadas estão promovendo melhorias nos processos administrativos e/ou operacionais realizados pelos órgãos. Além disso, as perspectivas dos órgãos indicam que as soluções de IA utilizadas têm auxiliado os agentes governamentais a oferecerem melhores serviços públicos aos cidadãos, permitindo a efetividade da ação governamental, elemento fundamental para fortalecer a democracia.

#### **4.4 Riscos democráticos que envolvem o uso de IA na gestão pública**

Como discutido, o uso de IA na gestão pública pode oferecer benefícios para a democracia, a partir do seu potencial para contribuir para o aumento da eficiência na máquina pública, ao auxiliar na entrega de serviços de maior qualidade aos cidadãos e com uma abordagem inovadora para melhor cumprimento dos direitos sociais. Contudo, é imperioso salientar que, mesmo ao explorar os avanços da inteligência artificial, a gestão pública deve, acima de tudo, aderir aos princípios fundamentais do Estado Democrático de Direito. Como visto no Referencial Teórico, a IA pode reproduzir diversos comportamentos da sociedade, e incorporar vieses discriminatórios. Dessa forma, a eficiência proporcionada pela inteligência artificial não pode ser alcançada às custas dos direitos fundamentais, uma vez que qualquer ameaça significativa a esses direitos representa um risco substancial à democracia. Cabe, assim, apontar os principais riscos à democracia que as ferramentas baseadas em IA utilizadas pela gestão pública podem oferecer.

A opacidade dos algoritmos é uma grande preocupação, sendo fundamental garantir a transparência acerca da natureza dos algoritmos utilizados na gestão pública para que os cidadãos compreendam como as decisões são tomadas (ARAÚJO, ZULLO & TORRES, 2020; FORNASIER, 2021). Ademais, algoritmos podem incorporar vieses, muitas vezes refletindo discriminações e preconceitos da sociedade que são repassados aos dados usados para treiná-los, o que pode resultar

em decisões discriminatórias (ARAÚJO, ZULLO & TORRES, 2020; FORNASIER, 2021; COSTA & KREMER, 2022).

O suporte algorítmico à tomada de decisões desempenha uma função notável ao ajudar os agentes públicos a estabelecer ações que têm um impacto direto ou indireto na vida das pessoas, influenciando, assim, o exercício dos direitos fundamentais (BRASIL, 2020; ELIAS, 2021). A aplicação irresponsável dessas tecnologias pode acarretar impactos danosos no exercício dos direitos fundamentais pela sociedade, tais como o direito à privacidade, à proteção contra a discriminação, à presunção de inocência, ao acesso à justiça, à intimidade, às liberdades de expressão, dentre outros (BRASIL, 2020; ARAÚJO, ZULLO & TORRES, 2020; ELIAS, 2021). Como abordado no Referencial Teórico, iniciativas governamentais apoiadas em tecnologias que violem direitos fundamentais podem representar riscos substanciais à democracia, tendo em vista que afeta negativamente um dos tipos de participação dos cidadãos apresentado por Jaloto e Moreira (2023), que se refere ao exercício de direitos.

Elias (2021) traz como característica de uma sociedade democrática o cuidado para manutenção de direitos durante o desenvolvimento de novas tecnologias. Brasil (2020) sugere algumas práticas para eliminar ou mitigar os vieses dos algoritmos e dos dados que alimentam as tecnologias de IA. Uma delas diz respeito à necessidade de algoritmos com códigos abertos. Ainda, quando há restrição de acesso por motivos de sigilo, como em casos de Segredo de Justiça Criminal, Brasil (2020) recomenda que o poder público deve fornecer ao cidadão, no mínimo, informações sobre as variáveis de entrada e saída do modelo, bem como o tipo de algoritmo utilizado, além da realização regular de auditorias do desempenho do algoritmo, conduzidas por especialistas externos ao órgão público.

Nesse íterim, com base em critérios desenvolvidos por Brasil (2020), pretende-se, inicialmente, apontar os potenciais impactos negativos a direitos que determinada ferramenta de IA pode acarretar situações reais com base no seu “*output*”, isto é, no resultado que ela foi desenhada para entregar ou, ainda, caso ocorra um possível erro em seu funcionamento. Posteriormente, procurou-se evidenciar quais ações estão sendo realizadas para mitigar esses possíveis vieses.

**Tabela 3** - Direitos fundamentais a serem impactados pelo uso das iniciativas da gestão pública que utilizam recursos de IA

## Direitos Fundamentais a serem impactados pela natureza ou mau funcionamento da IA

<b>Ferramenta</b>	A.I Desk
<b>Impactos negativos a direitos</b>	As ferramentas de reconhecimento facial podem apresentar vieses, especialmente quando treinadas com conjuntos de dados que refletem desigualdades ou preconceitos existentes na sociedade. Um possível viés diz respeito ao não reconhecimento de pessoas negras, indígenas, amarelas ou então à associação enviesada de determinados grupos a atividades criminosas, impactando negativamente o direito ao tratamento igualitário. Considerando que a ferramenta foi tratada com a base nacional de arquivos com cenas de abuso sexual infantil, cabe analisar a diversidade de gênero, etnia e raça desta base para evitar possíveis vieses. A revisão humana não é realizada em todas as imagens. Nesse caso um possível erro de funcionamento impactaria negativamente, podendo deixar de identificar uma violação de direito fundamental da criança.
<b>Ferramenta</b>	D.E.I.A. - Defesa Econômica com Inteligência Artificial
<b>Impactos negativos a direitos</b>	O mau funcionamento do modelo pode impactar direitos de consumidores e das empresas alvo de investigação. Caso a ferramenta não identifique atos de concentração, pode haver prejuízos para o princípio da livre concorrência. Se não houver informações acerca dos critérios utilizados para sumarização dos documentos analisados pela ferramenta, pode haver erros na análise de atos de concentração.
<b>Ferramenta</b>	DataBricks
<b>Impactos negativos a direitos</b>	Como a ferramenta foi desenvolvida por empresa privada e comprada pelo setor público, não é possível verificar os critérios utilizados pelo algoritmo para manejo e atualização dos dados que alimentam a ferramenta. Isso impede que as etapas do processo de aprendizado de máquina que resultaram em ação por parte da ferramenta sejam rastreáveis e que as variáveis que pesaram na tomada de decisão sejam tornadas públicas. Tal fator pode violar o princípio da transparência. Além disso, não é possível verificar se todos os dados de bases governamentais que são compartilhados pelos órgãos e integrados pela ferramenta também serão acessados pela empresa fornecedora da ferramenta. Isso pode significar violação do direito à privacidade.
<b>Ferramenta</b>	Delphos
<b>Impactos negativos a direitos</b>	Tendo em vista que ferramentas de processamento de linguagem natural tendem a funcionar melhor com textos formais e bem escritos gramaticalmente e com poucos erros e abreviações, a ferramenta pode impactar negativamente pessoas marginalizadas, ferindo o direito à igualdade. O algoritmo pode se tornar enviesado contra pessoas de baixa renda que não possuem um bom domínio do português, ou que utilizam gírias e/ou termos informais.
<b>Ferramenta</b>	Localizador de Evidências Digitais (LED)

---

<b>Impactos negativos a direitos</b>	As ferramentas de reconhecimento facial podem apresentar vieses, especialmente quando treinadas com conjuntos de dados que refletem desigualdades ou preconceitos existentes na sociedade. Um possível viés diz respeito ao não reconhecimento de pessoas negras, indígenas, amarelas ou então à associação enviesada de determinados grupos a atividades criminosas, impactando negativamente o direito ao tratamento igualitário. Considerando que a ferramenta foi tratada com a base nacional de arquivos com cenas de abuso sexual infantil, cabe analisar a diversidade de gênero, etnia e raça desta base para evitar possíveis vieses. A revisão humana certamente não é realizada em todas as imagens. Nesse caso um possível erro de funcionamento impactaria negativamente, podendo deixar de identificar uma violação de direito fundamental da criança.
--------------------------------------	--

---

<b>Ferramenta</b>	NuDetective
-------------------	-------------

---

<b>Impactos negativos a direitos</b>	As ferramentas de reconhecimento facial podem apresentar vieses, especialmente quando treinadas com conjuntos de dados que refletem desigualdades ou preconceitos existentes na sociedade. Um possível viés diz respeito ao não reconhecimento de pessoas negras, indígenas, amarelas ou então à associação enviesada de determinados grupos a atividades criminosas, impactando negativamente o direito ao tratamento igualitário. Considerando que a ferramenta foi tratada com a base nacional de arquivos com cenas de abuso sexual infantil, cabe analisar a diversidade de gênero, etnia e raça desta base para evitar possíveis vieses. A revisão humana certamente não é realizada em todas as imagens. Nesse caso um possível erro de funcionamento impactaria negativamente, podendo deixar de identificar uma violação de direito fundamental da criança.
--------------------------------------	--

---

<b>Ferramenta</b>	PalasNET
-------------------	----------

---

<b>Impactos negativos a direitos</b>	As tecnologias de reconhecimento facial têm o potencial de impactar negativamente o princípio do tratamento igualitário, a depender do banco de dados utilizado para seu treinamento. Um possível viés emerge no não reconhecimento de pessoas não brancas, bem como na associação enviesada de determinados grupos a atividades criminosas. Além disso, as técnicas empregadas por essa ferramenta classificam indivíduos com maior ou menor probabilidade de levantar suspeitas, influenciando diretamente o curso das investigações. Adicionalmente, surge a preocupação com a custódia dos bancos de dados de imagens, uma vez que a biometria facial é considerada um dado pessoal sensível, e ainda carece de regulamentação específica.
--------------------------------------	--

---

<b>Ferramenta</b>	Projeto Cérebro
-------------------	-----------------

---

<b>Impactos negativos a direitos</b>	O modelo pode impactar direitos de consumidores, investidores e de outras empresas. Caso o mau funcionamento da ferramenta a leve a favorecer indevidamente uma empresa em detrimento das outras, isso pode resultar em uma violação da concorrência justa. Se a ferramenta envolver o processamento de dados sensíveis das empresas licitantes, pode haver preocupações com a privacidade e a proteção de dados.
--------------------------------------	---

---

<b>Ferramenta</b>	Sinesp Big Data
-------------------	-----------------

---

---

<b>Impactos negativos a direitos</b>	A coleta e armazenamento de dados sobre movimentação de veículos podem ser interpretados como uma invasão do direito à privacidade. Se o sistema for utilizado de forma a focar desproporcionalmente em determinadas comunidades ou grupos sociais, isso poderia constituir uma violação do princípio à igualdade. Se o sistema for utilizado para identificar veículos com base em suspeitas não comprovadas, isso pode violar o princípio da presunção de inocência.
--------------------------------------	--

---

<b>Ferramenta</b>	Sistema Alerta Brasil
-------------------	-----------------------

---

<b>Impactos negativos a direitos</b>	A coleta e armazenamento de dados sobre movimentação de veículos podem ser interpretados como uma invasão do direito à privacidade. Se o sistema for utilizado de forma a focar desproporcionalmente em determinadas comunidades ou grupos sociais, isso poderia constituir uma violação do princípio à igualdade. Se o sistema for utilizado para identificar veículos com base em suspeitas não comprovadas, isso pode violar o princípio da presunção de inocência.
--------------------------------------	--

---

<b>Ferramenta</b>	Sistema CórteX
-------------------	----------------

---

<b>Impactos negativos a direitos</b>	Por ser uma ferramenta voltada para vigilância por videomonitoramento, há o risco de identificação de alvos móveis suspeitos sem que tenha ocorrido, comprovadamente, alguma prática passível de penalização. A coleta e armazenamento de dados sobre movimentação de veículos e localização dos indivíduos podem ser interpretados como uma invasão do direito à privacidade. Se o sistema for utilizado de forma a focar desproporcionalmente em determinadas comunidades ou grupos sociais, isso poderia constituir uma violação do princípio à igualdade. Se o sistema for utilizado para identificar veículos com base em suspeitas não comprovadas, isso pode violar o princípio da presunção de inocência.
--------------------------------------	--

---

<b>Ferramenta</b>	Solução Automatizada de Identificação Biométrica (ABIS)
-------------------	---

---

<b>Impactos negativos a direitos</b>	Algoritmos de reconhecimento biométrico têm o potencial de impactar negativamente o princípio do tratamento igualitário, a depender do banco de dados utilizado para seu treinamento. Um possível viés emerge no não reconhecimento de pessoas não brancas, bem como na associação enviesada de determinados grupos a atividades criminosas. Como a ferramenta foi adquirida de empresa privada, não é possível afirmar que foi desenvolvida a fim de mitigar vieses. Erros na identificação biométrica podem resultar em acusações injustas, prejudicando o direito à presunção de inocência. Se os dados biométricos forem usados para fins não autorizados ou além do escopo inicialmente previsto, isso pode provocar violação do direito à privacidade. A coleta e armazenamento de dados biométricos, como impressões digitais e reconhecimento facial, podem representar uma ameaça à privacidade se não forem adequadamente protegidos. Por ser uma tecnologia comprada pronta, há falta de conhecimento acerca dos critérios utilizados para reconhecimento de padrões faciais por essa tecnologia, ou como funcionam os <i>inputs</i> nos bancos de dados. Isso impacta negativamente o princípio da transparência.
--------------------------------------	---

---

<b>Ferramenta</b>	Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa
-------------------	---

---

<b>Impactos negativos a direitos</b>	<p>A falha na identificação de transações suspeitas pelo algoritmo pode impactar negativamente o princípio do livre mercado.</p> <p>Algoritmos que analisam transações financeiras para identificar atividades suspeitas podem envolver a análise de dados pessoais e financeiros de investidores. Se não houver medidas adequadas para proteger a privacidade e a confidencialidade dessas informações, os direitos à privacidade podem ser comprometidos.</p> <p>Falhas de segurança podem resultar em vazamentos de informações sensíveis, como dados financeiros dos investidores, prejudicando a confiança dos investidores na ação reguladora do Estado.</p>
<b>Ferramenta</b>	Robô Glória
<b>Impactos negativos a direitos</b>	<p>Por se tratar de uma ferramenta que é destinada a um público específico, é importante entender se as meninas e mulheres que entram em contato com a ferramenta foram devidamente informadas com transparência sobre a finalidade da coleta dos dados e como estão sendo utilizados aqueles dados. Ou seja, é importante entender como foram armazenados os dados para a criação da base de dados para o público específico e se elas foram informadas deste armazenamento, caso contrário, este serviço cometerá um abuso quanto ao uso de informações pessoais dos seus usuários.</p> <p>Por se tratar de uma ferramenta baseada em <i>machine learning</i>, que aprende a cada interação, é importante que os desenvolvedores se atentem à possibilidade de o robô reproduzir ofensas ou comportamentos de pessoas má intencionadas que possam entrar em contato com a ferramenta.</p> <p>O receio com ferramentas de interação exclusivamente <i>online</i> reside na impossibilidade de acesso para indivíduos cuja inclusão digital tenha sido conduzida de maneira precária, incompleta ou inadequada, como analfabetos, imigrantes, pessoas com deficiência ou aqueles que não possuem acesso estável à internet.</p>

Fonte: elaboração própria, 2023.

Duas formas práticas a serem realizadas pela gestão pública para evitar a não violação de tais direitos pelo uso das ferramentas referem-se à supervisão humana das decisões automatizadas e à consideração de possíveis vieses em seu desempenho (BRASIL, 2020). Por meio de solicitações de acesso à informação feitas aos órgãos implementadores e pelo catálogo do Transparência Brasil de uso de IA no setor público, foi possível averiguar se tais ações são implementadas. Infelizmente, não foi possível obter tais dados acerca do Robô Glória.

As ferramentas que contam com obrigatoriedade de revisão humana das decisões automatizadas nas ferramentas A.I Desk, D.E.I.A, Delphos, LED, Nudetective, PalasNet, Sistema Alerta Brasil, ABIS e Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa. Já o Databricks, o Projeto Cérebro e o Sistema Córtex são ferramentas cujos órgãos implementadores informaram que, desenvolvimento e/ou implementação da ferramenta, não foi considerada a obrigatoriedade de revisão

humana das decisões automatizadas. Para mais, não foi possível obter essa informação em relação à ferramenta Sinesp Big Data, tendo em vista que o MJSP não respondeu a tal questão no pedido de acesso à informação enviado ao órgão. Dessa forma, a maioria das ferramentas conta com revisão das decisões automatizadas.

Ainda, os órgãos indicaram que, durante o processo de desenvolvimento/implementação dos algoritmos, apenas três (3) ferramentas consideraram possíveis vieses em seu desempenho, são elas: LED, Nudetective, e a Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa. Ademais, a PF informou que não detém conhecimento acerca desse aspecto no desenvolvimento da ferramenta ABIS, tendo em vista que a tecnologia foi comprada pronta. Tal fator corrobora com as ideias de Schuler & Montardo (2020), os quais apontaram para a falta de transparência no cenário brasileiro em relação aos contratos de fornecimento de sistemas de biometria facial. Não foi possível obter informação acerca da obrigação de revisão humana nas decisões automatizadas tomadas pela ferramenta Sinesp Big Data, uma vez que não houve resposta do MJSP referente a essa questão no pedido de acesso à informação enviado ao órgão.

A partir da noção de que a falta de transparência algorítmica também pode apresentar riscos democráticos, procurou-se averiguar se mecanismos de transparência estão sendo utilizados pelos órgãos do governo federal para mitigar os possíveis impactos negativos gerados pelas ferramentas de IA. Para análise dos dados, utilizou-se critérios baseados no Referencial Teórico. Estes critérios referem-se a:

1. Quais ferramentas possuem código aberto?
2. Para quantas ferramentas há realizações periódicas de auditorias do funcionamento do algoritmo, por órgãos fiscalizadores ou por especialistas externos ao órgão público?
3. De quais ferramentas é possível obter informações sobre suas variáveis de entradas e de saídas, além do tipo de algoritmo utilizado?
4. Quais ferramentas utilizam dados pessoais para o seu treinamento? Os órgãos especificam quais dados são utilizados?
5. Os órgãos do governo federal divulgam tais ferramentas em documentos disponíveis em meio eletrônico? É fácil compreender as ferramentas a partir

dos dados oferecidos pelo governo em meio eletrônico? As informações são acessíveis?

Em relação ao item 1, os dados coletados apontam que nenhuma ferramenta mapeada e analisada conta com código aberto. Apenas o Cade informou que o código da ferramenta D.E.I.A está em processo de abertura. Já no que diz respeito ao item 2, nenhum órgão indica a realização periódica de auditorias por órgãos fiscalizadores ou por especialistas externos ao órgão público acerca do funcionamento dos algoritmos. Isso é um fator bastante preocupante, tendo em vista que

Das 13 ferramentas, foi possível obter informações relativas às suas variáveis de entradas e de saídas, além do tipo de algoritmo utilizado, sobre sete (7), são elas: D.E.I.A, Delphos, LED, Nudetective, Sistema Alerta Brasil, Sistema Córtex e Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa. Acerca do Projeto Cérebro, foi possível verificar seu modelo estatístico, mas não foi possível tomar conhecimento das suas entradas e saídas. O contrário acontece com a ABIS; a PF declarou não dispor da informação acerca do modelo estatístico utilizado, pois foi adquirida de empresa privada e os fornecedores não tornaram tal informação pública. Porém, o órgão informou suas variáveis de entradas e de saídas. Os órgãos implementadores da A.I Desk, do Databricks, do PalasNet e do Sinesp Big Data não informaram tais dados acerca dessas ferramentas.

Em relação ao item 4, dentre as 13 ferramentas analisadas, dez (10) utilizam dados pessoais para treinamento, são elas: A.I Desk, D.E.I.A, Delphos, Nudetective, PalasNet, Sinesp Big Data, Sistema Alerta Brasil, Sistema Córtex, Solução Automatizada de Identificação Biométrica (ABIS) e Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa. Tais órgãos, contudo, não especificam quais dados pessoais são utilizados. As iniciativas LED e Projeto Cérebro indicam não utilizar dados pessoais, mas dados anonimizados. Não foi possível obter tal informação acerca da ferramenta DataBricks. Foi visto no Referencial Teórico que o treinamento de algoritmos pressupõe uma coleta massiva de dados, e em muitos casos, esses são dados pessoais.

Cabe ressaltar que o cidadão tem direito à proteção de seus dados pessoais e, por mais que estes estejam sendo utilizados no contexto de segurança pública, é necessário que haja transparência sobre como esses dados foram armazenados e

utilizados pelos órgãos governamentais (BRASIL, 2020). Contudo, tais informações não são tornadas públicas pelos órgãos implementadores, o que pode gerar práticas abusivas na gestão pública, como compartilhamento não autorizado de dados pessoais (ELIAS, 2021) e vigilância sem precedentes (DE ANDRADE et al, 2022). Isso é extremamente perigoso em um sistema democrático, tendo em vista que uma das características intrínsecas desse sistema consiste na garantia dos direitos constitucionais de intimidade, da privacidade e autodeterminação informativa como um direito individual (ELIAS, 2021).

Nesse contexto de permissão para uso de dados pessoais no âmbito da segurança pública, é interessante comparar as ferramentas utilizadas pelo governo federal com o algoritmo desenvolvido pela sociedade civil, o Robô Glória. Foi visto que as iniciativas governamentais que fazem uso de IA na área de segurança pública não divulgam como são armazenados e utilizados os dados pessoais, ou mesmo sensíveis, como é o caso do PalasNet, dos cidadãos. Por outro lado, na descrição da Glória foi possível verificar que, ao entrar em contato com a ferramenta, a robô pede dados como faixa etária, localização e dados socioeconômicos das vítimas, os quais são fornecidos de forma voluntária e passam por processo de anonimização<sup>59</sup>. Além disso, fica claro a finalidade do uso desses dados, que é gerar relatórios que ajudem na formação de políticas de combate à violência a partir de todos os detalhes que as vítimas contam para identificar perfis de quem sofre violência e padrão de ocorrências<sup>60</sup>. Com isso, percebe-se que a iniciativa da sociedade civil demonstra maior preocupação no tratamento de dados pessoais dos cidadãos do que o poder público.

Por fim, no que concerne à disponibilização de informações pelos órgãos do governo federal em meio eletrônico acerca das ferramentas, verificou-se que grande parte das ferramentas não ganha forte exposição e nem dispõem de muitos dados que possibilitam compreendê-las com clareza. Ademais, não há informações em portais governamentais acerca da A.I Desk, do Databricks, do Delphos, da Solução Automatizada de Identificação Biométrica (ABIS) e da Solução personalizada de

---

<sup>59</sup> Informações disponíveis em: <https://brasilpaisdigital.com.br/loria-projeto-de-plataforma-de-inteligencia-artificial-voltada-para-o-combate-a-violencia-contra-a-mulher/>. Acesso em 24 de novembro de 2023.

<sup>60</sup> Informações disponíveis em: <https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/comissao-de-defesa-dos-direitos-da-mulher-cmulher/noticias/lancamento-do-projeto-loria>. Acesso em 24 de novembro de 2024.

algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa. Já os dados disponibilizados sobre as ferramentas D.E.I.A, PalasNet, Sistema Alerta Brasil e Sistema Córtex são mais superficiais, não permitindo a compreensão completa acerca do funcionamento das ferramentas. Foi possível obter dados acerca do LED e do Nudetective por meio da edição 42 da Revista Perícia Federal, disponibilizada pela Associação Nacional dos Peritos Criminais Federais (APCF). Já as ferramentas com mais informações disponíveis em meio eletrônico pelos órgãos do governo federal foram a Sinesp Big Data e o Projeto Cérebro.

Ao apoiar-se nas ideias de Fornasier (2021), o qual aponta que um dos principais riscos do uso de IA pelo setor público refere-se a sua falta de transparência. O autor indica que, a coleta massiva de dados para alimentar os algoritmos leva a dois tipos de opacidade. A primeira é a opacidade técnica, a qual sugere a dificuldade que a maioria dos cidadãos apresentam para compreenderem a tecnologia por trás da coleta de dados em massa. A segunda refere-se à opacidade algorítmica, a qual resulta das propriedades intrínsecas a algoritmos que orientam a coleta e o processamento de dados em massa. A última torna complexo até mesmo para especialistas da área compreenderem como os dados são tratados pelos algoritmos. Isso indica que os órgãos deveriam agir no sentido de adoção de estratégias para tornar as informações acerca do uso dos algoritmos não só disponíveis, mas também mais acessíveis NOHORA E COLOMBO (2019).

Contudo, a dificuldade em obter informações acerca das iniciativas baseadas em algoritmos por meio de acessos a documentos disponibilizados em meio eletrônico e sites governamentais revela uma falta de transparência por parte dos órgãos, o que impede que o cidadão exerça controle social acerca do uso de seus dados pessoais, além de não proporcionar insumos para que se torne viável ao cidadão aferir os possíveis riscos a direitos que tais ferramentas podem oferecer, representando riscos à democracia. Foi possível obter dados mais aprofundados sobre a natureza das ferramentas por meio dos pedidos de acesso à informação feitos diretamente aos órgãos na plataforma Fala.br. Todavia, ao considerar que as informações acerca da existência das ferramentas ainda são bastante opacas, não há estímulos para que o cidadão realize controle social acerca dessas ferramentas, ou mesmo seja capaz de se preocupar com seus riscos. Nesse sentido, observou-se na maioria das ferramentas de IA analisadas o que se chamou pelas autoras de opacidade na gestão.

Com base nos dados coletados, nota-se que nem todos os instrumentos de transparência algorítmica são explorados pelos órgãos implementadores das iniciativas de IA analisadas. Até o momento de realização desta pesquisa, todas as ferramentas possuem código fechado, o que não surpreende tendo em vista que são iniciativas da área de Segurança Pública. Porém, a realização periódica de auditorias por especialistas externos ao órgão público, que é uma solução sugerida por Brasil (2020) para verificar a eficácia das ferramentas e para superar o problema da opacidade dos algoritmos indicada por Fornasier (2021), também não vem sendo realizada. Apesar de a maioria dos órgãos informarem as variáveis de saída e de entrada das ferramentas, além do modelo estatístico em que ela se apoia, deve haver somado a isso, mecanismos de controle institucional por parte de órgãos fiscalizadores ou mesmo de especialistas externos ao órgão público. Tal controle é essencial para averiguar se os algoritmos implementados são efetivos em relação a seus objetivos, se as decisões tomadas com seu apoio são legítimas e, até mesmo, se provocam algum impacto negativo a direitos fundamentais.

A ferramenta ABIS, por exemplo, é uma ferramenta cuja natureza algorítmica apresenta alta possibilidade de riscos discriminatórios. Como a ferramenta foi fornecida por empresa privada, a PF informou não ter informações acerca do modelo estatístico utilizado na ferramenta ou, ainda, se foram considerados vieses em seu desenvolvimento, o que é muito perigoso do ponto de vista democrático. Trata-se de uma ferramenta que se alimenta de dados pessoais sem o conhecimento dos cidadãos, tendo em vista que a PF não divulga informações acerca da ferramenta em *sites* ou documentos governamentais, o que contribui para sua opacidade algorítmica. Todos esses fatores contribuem para a falta de transparência algorítmica desta ferramenta, a qual impede o controle social e dos órgãos fiscalizadores e abre possibilidades para ocorrência de impactos negativos a direitos, além de não ser possível verificar se a ferramenta cumpre o propósito para o qual foi projetada. Tais fatores representam sérios riscos à democracia.

Outra ferramenta que merece atenção é o CórTEX. Como abordado anteriormente, trata-se de uma ferramenta que permite acesso a diversos bancos de dados com informações sigilosas e sensíveis de cidadãos e empresas. Sem mecanismos de transparência algorítmica, como código aberto e realização de auditorias de controle externo do desempenho do algoritmo, que é o que os dados desta pesquisa indicam, nada impede que o sistema possa ser usado para

monitoramento e vigilância de cidadãos em uma escala sem precedentes. Isso pode promover violações legais à intimidade e à privacidade, à liberdade de expressão e manifestação, ao devido processo legal e a diversas outras garantias fundamentais da pessoa humana, como a integridade física e psíquica e, até mesmo, à vida.

#### **4.5 Atuação do MCTI no monitoramento das ferramentas de IA voltadas para a área de Segurança Pública**

De acordo com o tratado no capítulo da Metodologia, pretendia-se enviar um questionário ao Ministério da Ciência, Tecnologia e Inovação (MCTI) como meio de obter dados acerca dos recursos de Inteligência Artificial implementados nos serviços públicos federais até 2022. A motivação para tal ação teve como referência a EBIA, documento elaborado pelo MCTI com:

o papel de nortear as ações do Estado brasileiro em prol do desenvolvimento das ações, em suas várias vertentes, que estimulem a pesquisa, inovação e desenvolvimento de soluções em Inteligência Artificial, bem como, seu uso consciente, ético e em prol de um futuro melhor. (BRASIL, 2021b, p. 2).

A EBIA busca oferecer uma visão de futuro acerca do uso de IA no Brasil e estabelece um conjunto de ações estratégicas que buscam aproximar o Brasil dessa visão. Uma das ações estratégicas voltadas para a aplicação da IA no setor público destacadas pelo documento consiste em “linha com o estabelecido na Estratégia de Governo Digital, implementar recursos de Inteligência Artificial em, no mínimo, 12 serviços públicos federais até 2022. (BRASIL, 2021b, p. 45). Além disso, outra ação estratégica do governo abordada na EBIA para o uso de IA na segurança pública diz respeito a “estabelecer mecanismos supervisores para monitorar o uso da IA para atividades de segurança pública”.

Com base em tais ações estratégicas, foi enviado ao MCTI um questionário via Fala.br em busca de informações acerca das iniciativas voltadas para a área de Segurança Pública que fazem uso de IA. Todavia, o órgão relatou fazer o acompanhamento da EBIA, mas dispor de um conhecimento limitado sobre as ações ocorridas em cada setor específico. O Ministério indicou que constam informações sobre o uso policial para reconhecimento facial, mas o órgão não possui detalhes sobre essas ações.

Ainda, foi feito o questionamento para aferir se ocorre uma supervisão do MCTI sobre os órgãos que adotem esses instrumentos no sentido de seguirem as recomendações expostas na EBIA. O MCTI, por sua vez, revelou que não. O órgão apontou para a sua falta de *expertise* nos diferentes campos como justificativa, além da falta de competência legal, como no caso de segurança pública. O Ministério informou apenas que busca ser um facilitador da adoção da tecnologia, bem como, na medida do possível, busca uma coordenação entre os atores envolvidos.

Por fim, indagou-se acerca da existência e do funcionamento de alguma iniciativa de auditoria externa que realizasse avaliações periódicas acerca dos códigos dos algoritmos utilizados nas ferramentas. O órgão, no entanto, não respondeu. Tais fatores indicam que o Ministério formulador da estratégia não acompanhou a ação estratégica abordada na EBIA voltada para monitoramento do uso de IA para atividades de Segurança Pública. Isso também demonstra um ponto fraco da EBIA, na qual há o estabelecimento de várias ações estratégicas, mas não há definição de atores responsáveis por executá-las e nem prazos para sua realização. Tal aspecto dificulta que o problema identificado na análise referente à opacidade na gestão seja superado.

#### **4.6 Limitações da Pesquisa e Agenda de Estudos Futuros**

Dentre as limitações que esta pesquisa apresentou, destaca-se a consideração apenas da percepção dos órgãos implementadores de IA para verificar se houve aumento de eficiência nos órgãos. Uma vez que não foi possível identificar outros agentes externos que pudessem fornecer dados embasados para essa análise. Outra limitação refere-se à abrangência das iniciativas voltadas para à Segurança Pública, uma vez que o presente estudo não foi capaz de contemplar todas, posto que a coleta de dados dependeu em grande parte das informações disponibilizadas em meio eletrônico, no qual é possível encontrar um universo de informações. Buscou-se evitar tal problema ao questionar o MCTI sobre o monitoramento das iniciativas, porém o órgão não forneceu tal informação. Ainda, é possível mencionar a falta de dados coletados acerca do Robô Glória, o que impossibilitou uma análise mais detalhada acerca desta ferramenta.

Por fim, pode-se dizer que este trabalho contribui para pavimentar o caminho para a urgência de pesquisas relacionadas ao tema de Inteligência Artificial no setor público brasileiro e seus principais riscos e benefícios. Segue sugestões de alguns temas potenciais que englobam tanto o campo de públicas como outras áreas, como ciências da computação, direito e ciências sociais:

- Estudar com mais profundidade o Robô Glória, trazendo as perspectivas das vítimas ajudadas a fim de verificar seus efeitos para o combate à violência contra a mulher;
  - Investigar se o objetivo do Robô Glória de gerar relatórios com segmentação por faixa etária, local, dados socioeconômicos e padrão de ocorrências vem sendo realizado e, caso sim, se estes são utilizados para auxiliar o poder público na formação de políticas, projetos e ações para combater a violência contra a mulher;
  - Aferir as consequências éticas da reprodução de vieses dos algoritmos na área de Segurança Pública;
  - Estudar a importância da regulação do uso de IA pela gestão pública;
  - Realizar análise comparativa entre os dados dos estados que adotam as tecnologias de IA e os que não adotam a fim de aferir sua eficácia. Por exemplo, um estudo que ateste se os estados que aderiram ao Alerta Brasil apresentam de fato redução ou não nos índices de criminalidade;
  - Identificar tendências de ações estratégicas de governos estrangeiros a serem adotadas por órgãos fiscalizadores para aferir os resultados das ferramentas de IA;
  - Analisar o processo de desenvolvimento de Inteligência Artificial pelos órgãos no setor público;
  - Analisar o processo de implementação de cada ferramenta separadamente, identificando as ações concretas promovidas por eles bem como a mudança na qualidade do serviço público a partir de sua utilização;
  - Proposição de indicadores para medir a eficácia das ferramentas de reconhecimento facial utilizadas pelos órgãos de segurança pública no Brasil;
- e

- Analisar os riscos legais à democracia promovidos pelas ferramentas de videomonitoramento e de reconhecimento facial utilizados pelos governos estaduais e municipais no Brasil.

## 5 Considerações Finais

Este trabalho se propôs a identificar e analisar as iniciativas de IA utilizadas na gestão pública para a área de segurança pública em nível federal no Brasil e, a partir disso, investigar seus potenciais riscos e benefícios à democracia. Neste sentido, procurou-se realizar uma discussão acerca de conceitos fundamentais para subsidiar a análise, como democracia e o uso de tecnologias, tecnologias e eficiência na gestão pública, inteligência artificial e sua aplicação na gestão pública.

A democracia, neste estudo, foi simplificada apresentada a partir da linha teórica pluralista de Robert Dahl, o qual indicou que as ações de um governo democrático devem atender às preferências e demandas dos cidadãos, de modo a preservar seus direitos garantidos de forma legítima. Para isso atingir isso, observou-se que governos ao redor do mundo recorrem a mecanismos baseados em Inteligência Artificial para transformar a administração pública com o intuito de gerar benefícios significativos em termos de eficiência, transparência, participação cidadã e tomada de decisão. O uso de IA para gerar aumento de eficiência na gestão pública foi compreendido como benefício democrático, uma vez que se entendeu a eficiência como busca por melhores métodos no agir governamental que atendam cada vez melhor as demandas sociais, de modo a garantir a efetividade de direitos fundamentais e fortalecer, assim, a democracia. Assim, caso a IA seja capaz de proporcionar melhores métodos em processos administrativos e/ou operacionais na gestão pública, a ferramenta contribuirá para o aperfeiçoamento na entrega de serviços dos cidadãos, o que fortalece a democracia.

Todavia, autores como Silveira (2019), Elias (2021), Magrani (2021) e De Andrade et al (2022) indicam as preocupações com o uso dessas tecnologias pela gestão pública e seus potenciais riscos à democracia. Tais tecnologias podem estruturar uma reconfiguração das relações de poder na sociedade de modo a favorecer determinados grupos e ameaçar a igualdade de tratamento perante a lei. Isso ocorre, por exemplo, no processo de transmissão de vieses humanos para os algoritmos. Outra grande preocupação com o uso de IA refere-se a sua falta de transparência no processo de tomada de decisão pública, a qual pode comprometer a legitimidade democrática da ação estatal resultante de tal decisão. Neste aspecto, foi visto que os algoritmos, por natureza, apresentam potencial para impactar

negativamente direitos fundamentais, como privacidade, intimidade, tratamento igualitário, acesso à informação, proteção de dados pessoais, presunção de inocência, entre outros. Como visto, a garantia de direitos é essencial para manutenção de um ambiente democrático, e ferramentas que possam impactar negativamente direitos apresentam riscos à democracia.

Quanto aos métodos de pesquisa adotados, a coleta de dados combinou métodos quantitativos e qualitativos. Em seu delineamento pode ser classificada como uma pesquisa exploratório-descritiva. Foram utilizados tanto dados primários quanto secundários, como os questionários enviados aos órgãos do governo público federal por meio da plataforma Fala.br, as informações disponibilizadas em meio eletrônico por revistas digitais, a análise de documentos elaborados pelo poder público e a análise bibliográfica.

Por meio do objetivo específico I e II, foi possível identificar quatorze (14) iniciativas voltadas para área de Segurança Pública, sendo treze (13) implementadas pelo governo federal e uma (1) idealizada e implementada por uma organização da sociedade civil em parceria com o governo federal com apoio de outras empresas privadas.

No que tange ao objetivo específico III, foi possível descrever e caracterizar as iniciativas do governo federal com base nas respostas dos órgãos aos pedidos feitos pela plataforma Fala.br, nas informações presentes em documentos governamentais disponibilizados em meio eletrônico e nos dados oferecidos pela organização da sociedade civil Transparência Brasil, a qual elaborou um catálogo do uso de IA no poder público com base em informações fornecidas por órgãos governamentais.

Nessa etapa, foi possível perceber um desalinhamento entre as informações cedidas pelos órgãos às autoras desta pesquisa e outros dados disponibilizados em meio eletrônico acerca das ferramentas A.I Desk, PalasNet e Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa. Apesar das evidências que existem, ou existiram, as ferramentas A.I Desk e Solução personalizada de algoritmo para identificação de operações suspeitas realizadas nos mercados organizados de bolsa, seus órgãos implementadores negaram ter conhecimento a respeito dessas iniciativas. Além disso, ao ser questionado sobre a finalidade do PalasNet, o Departamento Penitenciário Nacional em momento algum mencionou que a ferramenta utiliza técnicas de reconhecimento facial, ao contrário do trazido pelo Transparência Brasil em seu

documento *Recomendações de Governança: uso de inteligência artificial pelo poder público*, utilizado como base no Referencial Teórico desta pesquisa. Tal desalinhamento foi tratado como opacidade na gestão por parte dos órgãos governamentais, na qual os próprios órgãos públicos não são capazes de trazer esclarecimentos sobre seus próprios instrumentos tecnológicos utilizados.

Em relação ao quarto objetivo específico, foi possível apresentar dados relativos ao desempenho e aos resultados alcançados por sete (7) ferramentas dentre as quatorze mapeadas. São elas o Localizador de Evidências Digitais (LED), o Nudetective, o A.I Desk, o Sistema Alerta Brasil, o Sistema Córtex, o Projeto Cérebro e o Delphos. Apesar de haver apenas dados que apontam para bons resultados e boa performance dos instrumentos, é preciso ressaltar que tais dados foram colhidos e disponibilizados pelos próprios órgãos implementadores das iniciativas que utilizam recursos de IA. O interessante seria que houvesse pesquisas feitas pelo Ministério Público ou pelo Tribunal de Contas da União (TCU), ou mesmo por outros membros da sociedade civil, que indicassem os resultados dos órgãos a partir do uso das ferramentas. Contudo, não foi possível encontrar nenhuma avaliação dessas organizações acerca das ferramentas, o que torna a pesquisa enviesada, e necessita de novos estudos que tratem tais variáveis.

Ademais, aferiu-se, a partir do ponto de vista dos órgãos implementadores, se as ferramentas já utilizadas foram capazes de contribuir para melhorias em processos administrativos e/ou operacionais dos órgãos; e se elas colaboram para que os agentes públicos desempenhem melhor a sua rotina e, assim, sejam capazes de entregar bens e serviços com mais qualidade aos cidadãos. Os resultados indicaram que a maioria das ferramentas de IA empregadas estão sendo capazes de promover melhorias nos processos administrativos e/ou operacionais ao trazer ganhos de produtividade; automatização e sistematização de processos administrativos que antes eram realizados de maneira manual; economia de tempo e de recursos; integração de dados entre diferentes órgãos; processamento mais ágil de análise de dados; e atualização automática de dados. Além disso, as perspectivas dos órgãos contribuíram para verificar que as soluções de IA utilizadas têm auxiliado os agentes governamentais a oferecerem melhores serviços públicos aos cidadãos, permitindo a efetividade da ação governamental, elemento fundamental para fortalecer a democracia. Tais fatores corroboram com as ideias trazidas no Referencial Teórico sobre aumento de eficiência.

Por outro lado, o objetivo específico V consistia em analisar os possíveis riscos do uso dos artefatos de IA à democracia. Ficou claro que, em um Estado Democrático de Direito, como é o caso do Brasil, a eficiência possibilitada pela inteligência artificial não pode ser alcançada às custas dos direitos fundamentais. Com isso, foi possível, por meio de pesquisa bibliográfica e documental, apontar os potenciais impactos negativos a direitos que as ferramentas de IA podem acarretar situações reais com base no seu *output* ou, ainda, caso ocorra um possível erro em seu funcionamento. Com isso, buscou-se investigar se ações voltadas a evitar a não violação de tais direitos pelo uso das ferramentas está sendo utilizadas pelos órgãos públicos. Ademais, foi possível averiguar se mecanismos de transparência estão sendo empregados pelos órgãos do governo federal, tendo em vista que a falta de transparência algorítmica representa um dos principais riscos à democracia oferecido pelo uso de IA na gestão pública.

Os resultados indicaram que, no processo de desenvolvimento/implementação dos algoritmos, apenas três ferramentas consideraram possíveis vieses em seu desempenho, o que é bastante alarmante. Já sobre ferramentas que contam com revisão humana obrigatórias das decisões automatizadas, os resultados apontam para nove (9) de quatorze (14) ferramentas, sendo que não foi possível obter tal dado sobre o Robô Glória. Além disso, verificou-se que poucas ações voltadas para trazer transparência algorítmica das iniciativas estão sendo realizadas pelos órgãos implementadores. Entende-se que, por se tratar de ferramentas voltadas para segurança pública, a divulgação externa possa favorecer estratégias de agentes externos mal-intencionados. Conforme tratado, o poder público, contudo, deve garantir a existência de mecanismos de transparência e *accountability* para que a sociedade civil possa exercer controle social na utilização de ferramentas baseadas em IA. No entanto, os dados analisados revelam que não é realizado nenhum tipo de monitoramento, avaliação ou auditoria das ferramentas por especialistas para averiguar se os algoritmos são eficazes em relação ao seu propósito e se ocasionam algum impacto negativo a direitos fundamentais. Isso é muito alarmante do ponto de vista democrático, tendo em vista a ausência de mecanismos de controle e fiscalização para determinar se há casos abusos de poder baseados na manipulação de algoritmos pela gestão pública.

A partir do exposto, este trabalho contribuiu para o avanço no campo científico de gestão de políticas públicas ao identificar o problema da opacidade na gestão em

relação à implementação de algoritmos. Isso revelou um grande problema ligado à falta de transparência, na qual os órgãos públicos não tornam públicas as informações acerca do uso de IA para os cidadãos e são incapazes de trazer esclarecimentos sobre ferramentas cujas evidências apontam para sua existência, como é o caso da A.I Desk, da Polícia Federal. Ademais, é importante reforçar que, para garantir que a democracia seja fortalecida, a eficiência na gestão pública possibilitada pela inteligência artificial, mesmo que haja comprovação mais prática de sua eficácia, não pode ser alcançada às custas dos direitos fundamentais. Em relação às contribuições práticas para a gestão pública, este trabalho apresentou possíveis práticas que a serem adotadas para mitigar os efeitos nocivos que podem ser oferecidos pelos algoritmos, como impactos negativos a direitos fundamentais. Além disso, contribuiu para identificar gargalos presentes na gestão pública atual. Foi possível também indicar ações a serem tomadas pelo poder público para garantir a transparência pública e o uso responsável de ferramentas baseadas em IA pelos órgãos governamentais de forma a procurar avançar no desafio relacionado à opacidade algorítmica.

## 6 Referências

ABRUCIO, Fernando Luiz; LOUREIRO, Maria Rita. Burocracia e ordem democrática: desafios contemporâneos e experiência brasileira. 2018.

ADDOR, Felipe. **Teoria Democrática e Poder Popular na América Latina**. Florianópolis: Editora Insular, 2016.

ARAGÃO, Cecília Vescovi de. Burocracia, eficiência e modelos de gestão pública: um ensaio. 1997.

AVRITZER, Leonardo. **Participatory Institutions in Democratic Brazil**. Johns Hopkins University Press, 2009.

BRANDÃO, Soraya Monteiro; BRUNO-FARIA, Maria de Fátima. Inovação no setor público: análise da produção científica em periódicos nacionais e internacionais da área de administração. *Revista de Administração Pública*, v. 47, p. 227-248, 2013.

BRASIL, Daniel Alves. O policiamento orientado pela inteligência e o desempenho da Polícia Rodoviária Federal na apreensão de drogas. 2022.

BRASIL, Decreto no 218, de 21 de setembro de 2021a. Dispõe sobre a Plataforma Integrada de Operações e Monitoramento de Segurança Pública - CórTEX. Brasília, DF, set.

BRASIL, Ministério da Ciência, Tecnologia e Inovações. Estratégia Brasileira de Inteligência Artificial. 6 abr. 2021b.

BRASIL, TRANSPARÊNCIA. Recomendações de governança: uso de inteligência artificial pelo poder público. **São Paulo**, 2020.

BOTELHO-FRANCISCO, RODRIGO EDUARDO; ORLANDO, ALEX FERNANDO. Investigações e experimentações em softwares para gestão de mídia no domínio do jornalismo: relato sobre interfaces de programação de aplicações. **Revista Brasileira de Ensino de Jornalismo**, v. 5, n. 16, p. 8-8, 2015.

CÓBE, Raphael MO et al. Rumo a uma política de Estado para inteligência artificial. **Revista USP**, n. 124, p. 37-48, 2020.

BRESSER-PEREIRA, Luiz Carlos. Reflexões sobre a reforma gerencial brasileira de 1995. *Revista do Serviço Público*. Brasília. v. 50, n. 4, p. 5-29. out-dez 1999. Disponível em: <https://revista.enap.gov.br/index.php/RSP/article/view/354>. Acesso em: 19 mai. 2023.

CAMPOS, S.L.B; FIGUEIREDO, J.M.. Aplicação de Inteligência Artificial no Ciclo de Políticas Públicas. **Cadernos de Prospecção**. V.15, p. 196-214, 2022.

CASTELLS, Manuel. Ruptura: a crise da democracia liberal. São Paulo: Zahar, 2018.

COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: Desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. **Revista Brasileira de Direitos Fundamentais & Justiça**, v. 16, n. 1, 2022.

DA SILVA, Rafaela Carolina; OTTONICAR, Selma Letícia Capinzaiki; YAFUSHI, Cristiana Aparecida Portero. A competência em informação e midiática voltada à cidadania: o uso da informação governamental para a participação na democracia. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 15, n. 3, p. 604-628, 2017.

DA SILVA, Washington Fernando; SILVA, Fernando Selleri; DA SILVA RABÊLO, Oliven. Tendências no uso de inteligência artificial e sua influência na requalificação da força de trabalho no setor público. *Cadernos de Prospecção*, v. 14, n. 3, p. 824-824, 2021.

DA SILVEIRA, Sergio Amadeu. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais**. Edições Sesc, 2017.

DAHL, R. A. *On democracy*. New ed.: New Haven, 1998.

DAHL, R. A. *Poliarquía*. São Paulo: Edusp, 1997

DE ALMEIDA, Layssa Ramos Maia; BAUTISTA, Judith Bustamante; ADDOR, Felipe. Potencialidades e limites do uso da tecnologia para o aprofundamento da democracia. **Revista Tecnologia e Sociedade**, v. 13, n. 27, p. 208-226, 2017.

DE ANDRADE, Otávio Morato et al. *A governamentalidade algorítmica: novos desafios para a democracia na sociedade da informação*. 2022.

DE ARAUJO, Valter Shuenquener; ZULLO, Bruno Almeida; TORRES, Maurílio. Big data, algoritmos e inteligência artificial na administração pública: reflexões para a sua utilização em um ambiente democrático. **A&C-Revista de Direito Administrativo & Constitucional**, v. 20, n. 80, p. 241-261, 2020.

DE DEFESA ECONÔMICA, Conselho Administrativo et al. *Prevenção e detecção de Cartéis em Licitações*. 2019.

DE LAAT, Paul B. *The disciplinary power of predictive algorithms: a Foucauldian perspective Ethics and Information Technology* Groningen Springer Berlin Heidelberg, 2019.

DE MENEZES, Cyntia Souza; SANLLEHÍ, José Ramon Agustina. BIG DATA, INTELIGÊNCIA ARTIFICIAL E POLICIAMENTO PREDITIVO: BASES PARA UMA ADEQUADA REGULAÇÃO LEGAL QUE RESPEITE OS DIREITOS FUNDAMENTAIS. **Novos Estudos Jurídicos**, v. 26, n. 1, p. 103-135, 2021.

DE SOUSA, Geovane Gomes et al. Monitoramento de segurança em uma cidade inteligente. *Revista Científica Redes de Computadores*, v. 3, n. 1, p. 28-38, 2023.

DESOUZA, Kevin C.; JACOB, Benoy. Big data in the public sector: Lessons for practitioners and scholars. *Administration & society*, v. 49, n. 7, p. 1043-1064, 2017.

DESORDI, Danubia; DELLA BONA, Carla. A inteligência artificial e a eficiência na administração pública. *Revista de Direito*, v. 12, n. 2, p. 1-22, 2020.

DI PIETRO, M.S.Z. *Direito Administrativo*. 18. ed. São Paulo: Atlas, 2005.

DIAS, Thiago Ferreira; SANO, Hironobu; MEDEIROS, Marcos Fernando Machado de. *Inovação e tecnologias da comunicação e informação na administração pública*. 2019.

DYE, T. R. *Understanding public policy*. Upper Saddle, NJ: Prentice Hall, 2005.

ELIAS, Paulo Sá. Algoritmos e inteligência artificial exigem atenção do Direito. *Revista CONJUR*, v. 20, 2021.

FONSECA, J. J. S. *Metodologia da pesquisa científica*. Fortaleza: UEC, 2002. Apostila.

FORNASIER, Mateus de Oliveira. *Inteligência artificial e democracia: oportunidades e desafios*. 2021.

FOUNTAIN, J. E. *Building the Virtual State: Information Technology and Institutional Change*. **Brookings Institution Press**, 2001.

FREITAS, Christiana Soares; SAMPAIO, Rafael Cardoso; AVELINO, Daniel Pitangueira de. *Proposta de análise tecnopolítica das inovações democráticas*. 2023.

GABARDO, Emerson. Princípio da eficiência. In: NUNES JUNIOR, Vidal Serrano et al. **Enciclopédia Jurídica da PUCSP, tomo II** (recurso eletrônico): direito administrativo e constitucional. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017.

GABRIEL, Martha. *Você, eu e os robôs: pequeno manual do mundo digital*. **São Paulo: Atlas**, 2018.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. São Paulo: Atlas, 2010.

GOMES, Elisabeth; BRAGA, Fabiane. **Inteligência Competitiva em tempos de Big Data: Analisando Informações e Identificando Tendências em Tempo Real**. Rio de Janeiro: Alta Books, 2017.

GOMES, Paulo; MARTINHO, José. RECURSOS HUMANOS NA ERA DA QUARTA REVOLUÇÃO INDUSTRIAL: REVISÃO SISTEMÁTICA DA LITERATURA SOBRE COMPETÊNCIAS PARA A INDÚSTRIA 4.0. **RAE-Revista de Ativos de Engenharia**, v. 1, n. 1, p. 17-29, 2023.

GONÇALVES JUNIOR, João Fernandes. Análise dos painéis de business intelligence construídos para subsidiar decisões estratégicas do sistema de GED SAPIENS na advocacia-geral da união. **Gerência de Projetos de Tecnologia da Informação-Unisul Virtual**, 2017.

GUIMARÃES, Tomás de Aquino; MEDEIROS, Paulo Henrique Ramos. A relação entre governo eletrônico e governança eletrônica no governo federal brasileiro. **Cadernos EBAPE-FGV**, Volume III, Número 4, Dez/2005.

HAMELINK, Cees J. New information and communication technologies, social development and cultural change. **URISD Discussion Paper**, 1997.

JALOTO, Tatiane Leal; DE SOUZA MOREIRA, Rafael Bezerra. Participação e controle sociais como instrumentos de fortalecimento da democracia: uma revisão de literatura. **Revista Mosaico**, v. 14, n. 1, p. 138-148, 2023.

JUNIOR, Iلسon Oliveira; DOS SANTOS, Franck Cione Coelho. INTELIGÊNCIA ARTIFICIAL E POLICIAMENTO PREDITIVO: possibilidades de inovação tecnológica para a Polícia Militar do Paraná no enfrentamento aos crimes violentos contra o patrimônio com emprego de explosivos. **Brazilian Journal of Technology**, v. 5, n. 1, p. 030-062, 2022.

KLUMB, Rosangela; HOFFMANN, Micheline Gaia. Inovação no setor público e evolução dos modelos de administração pública: o caso do TRE-SC. **Cadernos Gestão Pública e Cidadania**, v. 21, n. 69, 2016.

KRUG, Ana Paula Cordeiro; LEAL, Rogério Gesta. O CONTROLE SOCIAL POR MEIO DA TRANSPARÊNCIA ATIVA E PASSIVA NO ENFRENTAMENTO À CORRUPÇÃO: SOCIAL CONTROL THROUGH ACTIVE AND PASSIVE

KUZIEMSKI, Maciej; MISURACA, Gianluca. AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. **Telecommunications policy**, v. 44, n. 6, p. 101976, 2020.

LOPES, Luckas Sabioni; TOYOSHIMA, Silvia Harumi. Evidências do impacto da corrupção sobre a eficiência das políticas de saúde e educação nos estados brasileiros. **Planejamento e Políticas Públicas**, n. 41, 2013.

MACEDO, Joao; COSTA, Filipe; DOS SANTOS, Jefersson A. A benchmark methodology for child pornography detection. In: **2018 31st SIBGRAPI Conference on Graphics, Patterns and Images (SIBGRAPI)**. IEEE, 2018. p. 455-462.

MAGRANI, Eduardo. **Entre dados e robôs**. BOD GmbH DE, 2021.

MAIER, R., & SCHOLL J. (2017). Transformação digital do governo: avançando na inovação do setor público. **Government Information Quarterly**, 34(3), 387-391.

MANSBRIDGE, J. (2003). Rethinking Representation. *American Political Science Review*, 97(4), 515-528.

MEHR, Hila; ASH, H.; FELLOW, D. Artificial intelligence for citizen services and government. **Ash Cent. Democr. Gov. Innov. Harvard Kennedy Sch., no. August**, p. 1-12, 2017.

MEZZARROBA, Orides; BERNARDES, Marciele Berger. Democracia Eletrônica no Brasil: reflexões sobre o uso da internet nos processos eleitorais-Lei N.12034/09. In: **XIX Encontro Nacional do CONPEDI, 2010, Fortaleza, Anais**, p.3955-3964

MINAYO, M. C. S. Introdução. In: MINAYO, M. C. S.; ASSIS, S. G.; SOUZA, E. R. (Org.). **Avaliação por triangulação de métodos: Abordagem de Programas Sociais**. Rio de Janeiro: Fiocruz, 2010.

MOON, M. J. The Evolution of E-Government Among Municipalities: Rhetoric or Reality? **Public Administration Review**, 62(4), 424-433, 2002.

MORAIS, Janaina Jacolina. Princípio da eficiência na Administração Pública. **ETHOS JUS: revista acadêmica de ciências jurídicas**. Avaré: Faculdade Eduvale de Avaré, v. 3, n. 1, p. 99-105, 2009.

MOROZOV, Evgeny. Big Tech: a ascensão dos dados e a morte da política. São Paulo: Ubu Editora, 2018.

MULGAN, Geoff; ALBURY, David. Innovation in the public sector. London: Strategy Unit; Cabinet Office, 2003.

O'DONNELL, Guillermo. Teoria democrática e política comparada. **Dados**, v. 42, p. 577-654, 1999.

OCDE. Artificial intelligence in society. 2019. OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, 21 mai 2019

OLIVEIRA, Ana Maria Caldeira; IANNI, Aurea Maria Zöllner and DALLARI, Sueli Gandolfi. Controle social no SUS: discurso, ação e reação. **Ciênc. saúde coletiva** [online]. v. 18, n. 8, pp.2329-2338. 2013.

OLIVEIRA, Samuel. Sorria, você está sendo filmado! Repensando direitos na Era do reconhecimento facial. São Paulo: Thomson Reuters Brasil, 2021.

HARTMANN, Fabiano Peixoto; SILVA, Roberta Zumblick Martins da. Inteligência artificial e direito. 1. ed. Curitiba: **Alteridade**, 2019.

PRADHAN, Isha et al. Exploratory data analysis and crime prediction for smart cities. In: **Proceedings of the 23rd international database applications & engineering symposium**. 2019. p. 1-9.

PENCHEVA, Irina; ESTEVE, Marc; MIKHAYLOV, Slava Jankin. Big Data and AI—A transformational shift for government: So, what next for research?. **Public Policy and Administration**, v. 35, n. 1, p. 24-44, 2020.

PENITENCIÁRIA, Diretoria de Inteligência. A Atuação Da Diretoria De Inteligência Penitenciária (Dipen) No Âmbito Do Departamento Penitenciário Nacional. RBEP - Brasília, v. 3, n. 2, p. 279-295, jul./dez. 2022.

PEREIRA, Antonio Kevan Brandão. Teoria democrática contemporânea: as contribuições de Robert Dahl. **Sociologias Plurais**, v. 2, n. 2e, 2019.

PEREIRA, Breno Augusto Diniz; LOBLER, Mauri Leodir; DE OLIVEIRA SIMONETTO, Eugênio. Análise dos modelos de tomada de decisão sob o enfoque cognitivo. **Revista de Administração da UFSM**, v. 3, n. 2, p. 260-268, 2010.

PINTAUDI, S. M. Participação cidadã e gestão urbana. *Cidades*, São Paulo, v. 1, n. 2, 2004.

RIBEIRO, Manuella Maia; MEDINA, Javiera F.; LIMA, Luciana Piazzon B. Tecnologias emergentes e serviços digitais no setor público. 2022.

SABL, Andrew. The two cultures of democratic theory: Responsiveness, democratic quality, and the empirical-normative divide. **Perspectives on Politics**, v. 13, n. 2, p. 345-365, 2015.

SANTANA, C. L. Mecanismos de participación ciudadana para la planificación y evaluación de la gestión pública en el Ecuador. **Margen N**, v. 74, n. 02, 2014.

SANTANA, R. C. G. Mensuração da disponibilização de informações e do nível de interações dos ambientes informacionais digitais da administração municipal com a sociedade. Tese (Doutorado em Ciência da Informação) – Unesp, Marília, 2008.

SAVÉRIO, Natasja Alvarenga; NICOLAS, Maria Alejandra. O uso da inteligência artificial pela Administração Pública brasileira como ferramenta de controle institucional externo. **Encontro Brasileiro de Administração Pública**, 2022.

SILVA, Pedro Monteiro da; POLASTRO, Mateus de Castro. An overview of NuDetective Forensic Tool and its usage to combat child pornography in Brazil. In: **XLIII Jornadas Argentinas de Informática e Investigación Operativa (43JAIIO)-VI Workshop de Seguridad Informática (Buenos Aires, 2014)**. 2014.

SILVEIRA, Sérgio Amadeu da. Democracia e os códigos invisíveis – como os algoritmos estão modulando comportamentos e escolhas políticas. Edições Sesc, 2019.

SCHWAB, K.; The Fourth Industrial Revolution. **World Economic Forum**; Geneva, 2016.

SCHULER, Luis Gustavo Bier; MONTARDO, Sandra Portella. A política das máquinas: vieses em algoritmos de relevância pública. **Revista Tecnologia e Sociedade**, v. 16, n. 45, p. 300-312, 2020.

SELL, Carlos Eduardo. **Introdução à sociologia: política e sociedade na modernidade tardia**. Vozes, 2006.

SOARES, Ricardo Maurício Freire. A INFLUÊNCIA DO BIG DATA NO CONTROLE SOCIAL DA GESTÃO PÚBLICA THE INFLUENCE OF BIG DATE IN THE SOCIAL CONTROL OF PUBLIC MANAGEMENT. **REVISTA DIREITOS HUMANOS FUNDAMENTAIS OSASCO, SP ANO 18 N. 2 JUL./DEZ. 2018**, p. 83.

STAL, Eva. Inovação organizacional e tecnológica. **Inovação Tecnológica, Sistemas Nacionais de Inovação e Estímulos Governamentais à Inovação**, p. 23-53, 2007.

THE ECONOMIST INTELLIGENCE UNIT (EIU). Democracy Index 2021: *the China challenge?* 2021.

THE ECONOMIST INTELLIGENCE UNIT (EIU). Democracy Index 2022: *Frontline democracy and the battle for Ukraine*. 2022.

TRANSPARENCY IN COPING WITH CORRUPTION. **Revista Direito em Debate**, v. 30, n. 56, p. 6-13, 2021.

TRIVIÑOS, Augusto Nivaldo Silva. **Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação**. São Paulo: Atlas, 1987.

V-Dem Institute. Autocratization Changing Nature?. Democracy Report 2021. Gothenburg: V-Dem Institute, 2022.

VAN DE VEN, Andrew H.; ANGLE, Harold L.; POOLE, Marshall S. An introduction to the Minnesota innovation research program. In: VAN DE VEN, Andrew Harold; ANGLE, H. L.; POOLE, Marshall S. (Org.). Research on the management of innovation. The Minnesota studies. Nova York: Oxford University Press, 2000. cap. 1.

VAN NOORDT, Colin; MISURACA, Gianluca. Artificial intelligence for the public sector: results of landscaping the use of AI in government across the European Union. **Government Information Quarterly**, v. 39, n. 3, p. 101714, 2022.

VEALE, Michael; BRASS, Irina. Administration by algorithm? Public management meets public sector machine learning. **Public management meets public sector machine learning**, 2019.

VIGODA-GADOT, Eran et al. Public sector innovation for Europe: a multinational eight-country exploration of citizen's perspectives. *Public Administration Journal*, v. 86, n. 2, p. 307-329, 2008.

WARREN, Mark. What Can Democratic Participation Mean Today?. **Political Theory**, vol. 30, nº5, pp. 677-701, outubro, 2002.

WILNER, Alex S. Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation. **International Journal**, v. 73, n. 2, p. 308-316, 2018.

## Apêndices

### APÊNDICE A – QUESTIONÁRIO ENVIADO AO MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO

Na Estratégia Brasileira de Inteligência Artificial elaborada pelo Ministério da Ciência, Tecnologia e Inovações, consta na página 45 que uma das ações estratégicas seria "Em linha com o estabelecido na Estratégia de Governo Digital, implementar recursos de Inteligência Artificial em, no mínimo, 12 serviços públicos federais até 2022.". Com base nisso, gostaria de informações acerca das ferramentas já implementadas voltadas para a área de Segurança Pública. Se possível, gostaria de saber as seguintes informações acerca das ferramentas:

1. Nome da Ferramenta;
2. Órgão Implementador;
3. Qual o objetivo da ferramenta;
4. Com base nas recomendações da Estratégia Brasileira de Inteligência Artificial para o uso de instrumentos de IA para tomada de decisão, ocorre uma supervisão do MCTI sobre os órgãos que adotem esses instrumentos no sentido de seguirem tais recomendações?
5. Existe alguma iniciativa de alguma auditoria externa que realiza avaliações periódicas acerca dos códigos dos algoritmos utilizados nas ferramentas? Se sim, como funcionam essas auditorias? Elas são iniciativas de quais órgãos?

## APÊNDICE B - QUESTIONÁRIO ENVIADO AO INSTITUTO GLÓRIA

1. Qual o objetivo do Robô Glória?
2. Qual é a categoria de aplicação da ferramenta? Por exemplo, Classificação de imagens (exceto reconhecimento facial)/Reconhecimento facial/Sistema de recomendação/Chatbot/Estimativas de risco (incluindo detecção de fraudes/Análise de sentimentos/ Outros)?
3. Qual o modelo estatístico utilizado pelo Robô Glória? Por exemplo, Regressão logística/Regressão linear ou variações/Métodos baseados em árvore de decisão (incluindo florestas aleatórias e XGBoost)/Redes neurais/Processamento de linguagem natural/AutoML/Outros?
4. Quais são os outputs, ou resultados, da ferramenta? Por exemplo, probabilidade de determinado caso apresentar fraude; ou concessão ou não de crédito
5. Trata-se de uma inovação tecnológica desenvolvida pelo Instituto Glória? Ou foi comprada pronta? Se sim, de qual fornecedor?
6. Em relação à função da ferramenta, esta faz diagnósticos e toma decisões; faz diagnósticos e sugere ações; faz diagnósticos, mas não sugere ações? Há supervisão humana em todas as decisões sugeridas ou tomadas pelo algoritmo?
7. Em caso de erro do algoritmo corrigido por humano, essa informação é usada para aprimoramento do algoritmo?
8. A ferramenta pode impactar direitos fundamentais, seja por erro ou por design do seu algoritmo, seja direta ou indiretamente? Se sim, quais direitos fundamentais podem ser impactados?
9. Existem evidências de que este algoritmo alcance os objetivos para os quais ele está sendo utilizado? Caso sim, seria possível informar os objetivos comprovadamente alcançados?
10. Um comitê de ética acompanha/acompanhou o desenvolvimento do algoritmo e os ritos envolvidos na coleta e uso de dados?
11. No lançamento do projeto Glória realizado na Comissão de Defesa dos Direitos Humanos, é citado que um dos objetivos da Robô Glória seria gerar relatórios com segmentação por faixa etária, local, dados socioeconômicos e padrão de

ocorrências, com o intuito de auxiliar o poder público na formação de políticas, projetos e ações para combater a violência contra a mulher. Nesse sentido, tais relatórios estão sendo realizados? Se sim, eles são abertos ao público? Já foram utilizados pelo Poder Público?

12. O código da ferramenta é aberto? Se sim, como os usuários podem acessá-lo? Se não, há realizações periódicas de auditorias do funcionamento do algoritmo, por especialistas externos à empresa ou órgão público?
13. No desenvolvimento e/ou implementação da ferramenta, foram considerados possíveis vieses em seu desempenho? Por exemplo, sua eficácia é melhor com determinados grupos?
14. Se houve algum tipo de viés no desenvolvimento do algoritmo, os vieses foram corrigidos ou mitigados pelo código? De que maneira?
15. Foram feitos testes antes e durante a implementação para saber se taxas de erro são iguais ou menores em grupos minoritários?
16. A amostra de treinamento é rica em quantidade e diversidade para um bom resultado da ferramenta com os diferentes grupos aos quais a ferramenta é aplicada?