

VANTAGENS E RISCOS ENVOLVIDOS NO
EMPREGO DA INTELIGÊNCIA ARTIFICIAL
NA SEGURANÇA PÚBLICA

*ADVANTAGES AND RISKS INVOLVED IN
THE USE OF ARTIFICIAL INTELLIGENCE
IN PUBLIC SAFETY*

VANTAGENS E RISCOS ENVOLVIDOS NO EMPREGO DA INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA¹

ADVANTAGES AND RISKS INVOLVED IN THE USE OF ARTIFICIAL INTELLIGENCE IN PUBLIC SAFETY

Marcelo Gomes Maia Pires²

RESUMO

Este artigo analisa as vantagens e os riscos envolvidos na utilização da inteligência artificial na segurança pública, especialmente sua utilização prática por órgãos de segurança do Estado. Percebendo que se por um lado há vantagens evidentes no seu emprego, como a otimização de recursos, a agilidade no processamento de dados e a possibilidade de identificar padrões criminais, também se apresentam riscos e preocupações com questões éticas, existência de vieses presentes nos algoritmos e ameaças à privacidade dos cidadãos. Através de uma revisão bibliográfica e análise de experiências práticas em curso, concluiu-se que apesar dos desafios citados, com o uso responsável e regulamentado da IA, a tecnologia pode contribuir positivamente para a eficiência da segurança pública.

Palavras-chave: inteligência artificial; segurança pública; vantagens; desvantagens; vieses; privacidade.

1 INTRODUÇÃO

A inteligência artificial (IA) tem se tornado uma realidade em diversas atividades humanas, trazendo uma profunda mudança nas estruturas, perspectivas e potencialidades de praticamente todos os ramos de conhecimento atualmente existente.

¹ Data de recebimento: 11/03/2025. Data de aceite: 29/04/2025.

² Promotor de Justiça do Estado do Ceará, Especialista em Direito Público pela Universidade de Fortaleza, Direito Penal e Processo Penal pela Escola Superior do Ministério Público, Mestrando em Direito pela Universidade Unichristus. Email: marcelopires@mpce.mp.br. Currículo Lattes: <https://lattes.cnpq.br/6547140544389204>; ORCID: <https://orcid.org/0009-0001-0463-1585>.

A segurança pública não restou imune a esse fenômeno. Rapidamente se implementam diversas utilizações da IA no auxílio ou mesmo na completa substituição de agentes humanos empregados nesse ramo de atividade estatal, desde o policiamento, investigação e todas as demais fases da persecução penal. Mesmo hoje, quando não se pode mais ignorar que seu implemento está em irreversível tendência de crescimento, pode-se afirmar que a realidade e as estratégias policiais de combate ao crime já foram impactadas.

As experiências em curso possuem um objetivo em comum, qual seja, a maximização dos recursos do Poder Público com otimização dos resultados e redução dos custos. Como se sabe, o controle do conteúdo de comunicações de pessoas em vigilância, o reconhecimento facial usado para identificar indivíduos procurados pela Justiça ou mesmo a formulação de previsões estatísticas de locais mais propensos ao cometimento de crimes (apenas para citar alguns exemplos) são fundados num volume colossal de dados cuja análise, tratamento e produção de conhecimento só seria possível com a utilização de uma quantidade elevadíssima de pessoas e portanto de recursos financeiros.

A possibilidade de realizar mais, com contingentes reduzidos é apenas uma das muitas razões pelas quais o Estado vem lançando mão das facilidades que a IA proporciona, possibilitando a execução dessas tarefas.

Noutro giro, o debate sobre os limites éticos do uso da IA e a falta de transparência dessas iniciativas junto à opinião pública não acompanham o implemento de tais tecnologias na mesma velocidade em que elas emergem, assim subtraindo do debate público o necessário balanço comparatório entre e os ganhos e riscos envolvidos.

Tudo isso ganha especial contorno dramático quando se observa no discurso dos gestores e Agentes do Estado uma crença quase que religiosa na infalibilidade da máquina e por essa senda, dá-se um preocupante avanço nas liberdades civis de seus cidadãos.

Alguns estudiosos já começam a lançar o alerta: é preciso discutir os impactos, definir melhor as estratégias e procurar evitar (ou pelo menos reduzir ao máximo) a potencial violação de direitos e garantias fundamentais dos indivíduos, sem contudo restringir os benefícios que a IA trazem para a segurança da população.

Nas considerações a seguir analisaremos alguns exemplos do uso da inteligência artificial na segurança pública em nosso país e fora dele. Buscaremos pontuar criticamente alguns dos benefícios e lançaremos reflexões sobre os riscos envolvidos para contribuir com esse debate.

O estudo foi realizado com base em uma revisão bibliográfica, utilizando artigos acadêmicos, relatórios, material jornalístico e publicações de organizações que tratam do tema inteligência artificial e segurança pública, analisando tanto experiências no Brasil quanto em outros países, permitindo uma visão comparativa.

2 VANTAGENS DO USO DA IA NA SEGURANÇA PÚBLICA

Os primeiros resultados das experiências em andamento deixam bastante claro que a IA apresenta vantagens incontestáveis no seu emprego na Segurança Pública, melhorando substancialmente tanto a prevenção quanto o combate ao crime. As soluções nela baseadas têm sido utilizadas por órgãos de Estado com inegável sucesso para identificar e responder ao fenômeno criminológico com maior agilidade e precisão e, não raro, impactam positivamente os indicadores de violência e solução de casos.

As experiências que atualmente utilizam a nova ferramenta tecnológica são tão diversas quanto pulverizadas no Brasil e no mundo, de modo que não existem estatísticas precisas que mapeiem o número exato de projetos atualmente em andamento. Para se ter uma pequena ideia disso, basta que se diga que em março de 2023, pesquisadores ligados à Fundação Getúlio Vargas do Rio de Janeiro, publicaram estudo sobre as soluções de tecnologia mais utilizadas na segurança pública no Brasil, quando então que identificaram que os drones são adotados por 63% das forças de segurança, seguida das câmeras de reconhecimento de caractere ótico (tecnologia OCR³), com 44%. O reconhecimento facial também possui um grande destaque entre as ferramentas tecnológicas em utilização, estando presente em 33% do universo pesquisado, seguidas pelas câmeras nos uniformes dos policiais, que àquela altura já eram utilizadas por 22% das instituições policiais do país. Por fim, foi ainda identificado que o policiamento preditivo realizado por computadores para identificar áreas propensas à práticas criminais com base em dados passados, já era utilizado em 7% dos estados federados.⁴

Forçoso reconhecer que ainda são incipientes e estão em fase inicial as experiências que aliam o uso combinado de tecnologia e segurança pública no Brasil. Um dos exemplos em execução verificou-se em Santa Catarina, onde Polícia Militar tem utilizado ferramentas que otimizam os processos dentro da corporação e que vem servindo de modelo para outras cidades. Cuida-se da aplicação denominada PMSC Mobile, instalado em tablet, que substituem com eficiência os tradicionais formulários impressos e também combina as operações usualmente confiadas ao rádio transmissor. Essa simples iniciativa otimizou o atendimento de ocorrências policiais, com o registro de todos os dados colhidos diretamente no local, inclusive com coleta de áudio e vídeo que servirão como elementos de convicção relevantes, sendo concluído com a impressão do Termo Circunstanciado de Ocorrência aos envolvidos, poupando todo o tempo que seria destinado ao deslocamento às delegacias para confecção do procedimento (Sales, 2023. p. 87).

3 OCR é a sigla para *Optical Character Recognition*, ou Reconhecimento Ótico de Caracteres, tecnologia que permite converter imagens em texto codificado por máquina, capacitando-a a identificar letras, números e símbolos em uma imagem.

4 “Pesquisa analisa impacto das novas tecnologias na segurança pública”. Fundação Getúlio Vargas em: 11/04/2023 (<https://portal.fgv.br/noticias/pesquisa-analisa-impacto-novas-tecnologias-seguranca-publica>). Acesso em: 06 nov. 2024.

Em suas múltiplas aplicações que vão desde o reconhecimento facial de pessoas aos estudos sobre a probabilidade de ocorrência crime, passando pelo monitoramento de redes sociais e outras funcionalidades igualmente importantes, verifica-se que a IA tem se mostrado não apenas como uma tecnologia autônoma, mas também um complemento que potencializa várias outras soluções de segurança empregadas pelo Poder Público com grandes vantagens sobre os esforços antecedentes. Analisaremos a seguir alguns desses aspectos.

2.1 Otimização de Recursos e Eficiência Operacional

Em um cenário em que a gestão pública é desafiada por uma demanda cada dia mais crescente de oferta de serviços em um cenário de limitação de recursos do Erário a IA se destaca como um caminho natural para enfrentamento de um dos principais desafios que o Gestor público enfrenta, qual seja, a máxima potencialização do orçamento disponível.

O uso da nova tecnologia permite ao Estado melhorar a entrega de serviços, otimizar a alocação de recursos humanos e responder de forma mais rápida às necessidades da população na segurança pública com muito mais eficiência. Quando a IA realiza o gerenciamento de direcionamento de patrulhas policiais, monitora em tempo real grandes extensões territoriais identificando as principais áreas de alto risco, acaba por melhorar os esforços de para manter a cidade segura em benefício de todos.

Seja prevenindo a ocorrência de ocorrências criminosas, seja auxiliando cirurgicamente na localização e prisão de pessoas procuradas pela Justiça ou mesmo ajudando a coletar provas materialmente confiáveis de um crime cometido, a IA acaba contribuindo não apenas para um uso mais produtivo dos recursos humanos e financeiros do Estado, como também numa melhora do bem-estar social geral, com redução de números da violência.

2.2 Agilidade na Identificação de Padrões e Prevenção de Crimes

Diversas iniciativas que foram desenvolvidas no ambiente de aprendizado de máquina (*machine learning*) tornaram possíveis identificar padrões de ocorrências ilícitas e antecipar, com elevada margem de acerto, tendências à práticas criminais, assim permitindo uma atuação preventiva mais efetiva por parte das autoridades públicas ou ainda fornecendo suporte para a ação repressiva de forma mais direcionada.

As chamadas tecnologias de policiamento preditivo vem sendo empregadas para identificar, por meio de avaliações estatísticas, regiões ou indivíduos que podem repre-

sentar um maior risco à segurança pública, seja para justificar uma intervenção policial mais intensiva e direcionada, seja como instrumento de apoio para resolução de crimes já cometidos.

A vigilância decorrente do uso de IA no controle do espaço público pelas forças de segurança resta assim agigantado não apenas pela ampliação de sua dimensão territorial, mas também (e sobretudo) na precisão da resposta do Estado, que passa a ser direcionada para onde a necessidade de seu efetivo emprego se faz mais necessária.

Tarefas impossíveis a um agente humano dotado apenas dos recursos tradicionais, como detectar um veículo roubado numa rodovia repleta de milhares de automóveis, reconhecer um único indivíduo foragido da Justiça em meio a uma multidão de pessoas, torna-se perfeitamente possível com utilização desse tipo de suporte tecnológico

Até mesmo as iniciativas baseadas em premissas extremamente simples tem trazido impactos altamente positivos na Segurança Pública. Um exemplo eficaz do uso de IA vivenciada na cidade de Chicago nos EUA, que passou a utilizar maciçamente um *software* de policiamento preditivo denominado “*ShotSpotter*”, dotado de tecnologia capaz de capturar sons de tiroteios ocorridos em sua área territorial, avisando a polícia imediatamente de tais ocorrências, permitindo maior rapidez na presença das forças de segurança e do socorro médico nos locais apontados. Bada e Oliveira (2024) nos informam que nos anos subsequentes à adoção da tecnologia registraram-se quedas significativas de assassinatos.⁵ além da redução expressiva de tiroteios.

Como dito, a experiência de Chicago é fundada numa ocorrência rotineira na ocorrência de crime, qual seja, disparos de arma de fogo em área urbana. Não é difícil imaginar que o tempo de reação fundado nas respostas tradicionais, necessitando da percepção do fato e eventual colaboração da população com o Estado na comunicação da ocorrência e deslocamento dos agentes ao local não se compara à que consegue ser alcançada com o uso deste software. A desenvolvedora *SoundThinking* afirma que o *ShotSpotter* é “altamente preciso na detecção de tiros ao ar livre”, com uma taxa de precisão agregada de 97% entre os clientes que a utilizam, registrando uma taxa muito pequena de falsos positivos de menos de 0,5% de todos os incidentes de tiro relatados de 2019 a 2021.⁶

5 Segundo a polícia de Chicago, após a utilização da tecnologia houve uma diminuição de cerca de 13% nos assassinatos registrados em 2019, considerando aqueles ocorridos em 2018, além de uma queda de aproximadamente 35% em relação a 2016, quando Chicago relatou seu maior número de homicídios em duas décadas: 756. Os tiroteios também caíram. A contagem do departamento de polícia para o ano – 2.139 – é cerca de 9,6% menor que a contagem de 2.367 em 2018.

6 Consoante informações tiradas da empresa desenvolvedora do software - site <https://www.soundthinking.com/> (Acesso em: 12 nov. 24).

2.3 A Integração de Dados

Uma das maiores vantagens no uso de IA na segurança é a possibilidade de integração de dados oriundos de diferentes fontes, sejam elas públicas ou privadas, ligadas ou não à essa área específica da atuação. O uso de ferramentas fundadas em tecnologia AI, permitem a integração desses dados e conseguem automatizar tarefas complexas, simplificando todo o processo de produção de conhecimento, oferecendo ao Estado melhora na eficiência com redução dos custos.

Assim, os dados acumulados em bancos de dados alimentados ao longo de anos, em locais distintos planilhas linguagens e suportes variados, passam a ser compilados, processados e consequentemente utilizados como instrumento de melhora na capacidade de resposta das forças de segurança de forma muito mais ágil com o uso da IA. Isso possibilita uma visão mais precisa e abrangente da situação de segurança em tempo real.

Dados como registros criminais, informações oriundas de prestadoras de serviços públicos, elementos coletados em redes sociais e indicadores estatísticos urbanos, passam a produzir um conhecimento que orienta as decisões das autoridades públicas de forma muito mais rica, produzindo informações e conhecimento em tempo real.

Um exitoso exemplo desta integração é o sistema “Agilis”, implantado em 2021 pela Secretaria de Segurança Pública do Estado do Ceará, capaz de integrar inúmeros bancos de dados para fornecer informações aos agentes de segurança em tempo real. Os números são impressionantes, pegando-se por exemplo, a leitura de placas de veículos, instituição informa que o sistema realizou uma média diária de 5 milhões de reconhecimentos nos primeiros momentos de sua implantação. Nos 19 primeiros dias de maio do ano de 2021, o Agilis fez 216 mil leituras por hora. Em horário de pico, a tecnologia consegue ler simultaneamente até 300 placas por segundo⁷. Dados da própria secretaria informam que ações ostensivas e investigativas, realizadas com suporte desse tipo de tecnologia, resultaram no aumento de 24,8% nas capturas de pessoas realizadas pelas Forças de Segurança do Ceará, com 312 prisões e apreensões entre janeiro e agosto de 2024.⁸

3 RISCOS NO USO DA IA NA SEGURANÇA PÚBLICA

O crescente uso da IA na segurança pública também revelou problemas extremamente preocupantes que merecem a atenção imediata de legisladores, desenvolvedores

7 “COM integração de informações e base de dados, Agilis é lançado pela SSPDS como mais uma ferramenta de inteligência no combate ao crime”. Governo do Ceará. Fortaleza, 20 mai. 2021.

8 “AÇÕES das Forças da SSPDS resultam no aumento de 24,8% nas capturas por furto e receptação de fios em Fortaleza em 2024” Governo do Ceará. Fortaleza, 20 set. 2024.

e gestores públicos que decidem por sua utilização, revelando que a sociedade precisa debater de forma aberta e profunda a conveniência e oportunidade deste emprego.

Em lapidar reflexão, Mello (2023) nos adverte sobre esses riscos:

Uma vez que esses sistemas de IA são moldados por dados extraídos da realidade social como recursos audiovisuais, textos, dentre outras formas de externalização do comportamento relacional humano e, tendo em vista que essas informações têm como substrato realidades empíricas marcadas por múltiplos problemas estruturais relacionados às questões étnico-raciais, questões de ordem econômica, de gênero como condutas machistas, sexistas, misóginas, por questões que envolvem aspectos sobre as orientações sexuais em uma cultura heteronormativa, aduz-se que existe um grande risco da captura e utilização desses dados, para a manutenção do sistema hegemônico que molda as relações de poder e de dominação, ao fomentar formas de discriminação e de criminalização de determinadas pessoas ou grupos sociais em posições de vulnerabilidades. (2023).

Tudo isso vem causando profundas preocupações de estudiosos, que alertam para a necessidade de um debate mais aprofundado sobre os riscos envolvidos. Vejamos a seguir alguns desses aspectos em suas expressões e consequências.

3.1 Risco de Viés Preconceituoso e Discriminação Algorítmica

Antes de mais nada, é preciso lembrar que a IA é baseada em “algoritmos inteligentes ou algoritmos de aprendizagem”, em outras palavras, é composta por “um conjunto preciso de instruções ou regras, ou com uma série metódica de etapas que podem ser usadas para realizar cálculos, resolver problemas e tomar decisões” (Corvalán, 2017, p.299).

Ocorre que, a depender dos dados e *softwares* utilizados, esses sistemas inteligentes podem replicar aspectos da discricionariedade humana, dentre eles o viés preconceituoso.

Já são numerosos e variados os estudos que vem evidenciando a reprodução de vieses humanos no aprendizado de máquinas, não apenas replicando, mas até mesmo exacerbando preconceitos na produção das informações. Isso ocorre, por exemplo, quando um sistema de IA gera resultados que tratam determinados grupos ou etnias de forma desproporcional, seja para prejudicar ou para favorecer quando comparado ao tratamento dispensado aos demais, em um inaceitável padrão discriminatório.

Em que pese os algoritmos sejam pensados e projetados para processar dados de maneira objetiva, a realidade é que esses sistemas dependem do que lhe é inserido para “aprender”. O risco de viés se instala mais facilmente nesse momento, já que a eleição e a inserção desses dados muitas vezes são contaminados por premissas preconceituosas dos seres humanos que os elegeram e podem direcionar tendências autoritárias, sexistas, racistas, xenofóbicas e outras igualmente odiosas.

O problema é que, assim alimentados, os padrões contaminados por vieses passam a alimentar um círculo vicioso que levará à mais preconceito na atuação. Se um grupo específico passa a ser identificado como mais propenso à prática de crimes, por sugestão da IA recebe um maior número de abordagens policiais e, consequentemente, aumenta estatisticamente o número de ocorrências ligadas àquele grupo, o que naturalmente fará com que o padrão se confirme e se reforce, estimulando mais abordagens, repetindo o ciclo.

Pode-se assim dizer que as máquinas passam a reproduzir o chamado viés de confirmação entendido como fenômeno psicológico que consiste na tendência de procurar, interpretar ou criar novas evidências para que elas venham a validar crenças ou expectativas preexistentes (Mendonça, Silva 2023, p.98).

Já existem evidências sobranes de que aplicações de algoritmos de IA podem refletir vieses, replicando a discriminação que se origina dos próprios dados em que foram treinados, o que pode resultar em preconceitos e injustiças, afetando negativamente comunidades ditas marginalizadas. Em um contexto social complexo e multifacetado como o do Brasil essa questão pode ser especialmente complexa.

Realizando uma análise de alguns desses efeitos negativos, Mendes e Mattiuzzo (2019), concluíram que os padrões discriminatórios podem se manifestar sob diversas formas de manifestação, podendo se dar, até mesmo por erro estatístico (assim considerado quando os dados são coletados de forma incorreta ou tendenciosa) como podem decorrer de problemas ligados aos códigos dos algoritmos, que passam a realizar generalizações inaceitáveis baseadas em uma informação apenas parcial da realidade.

Pegando-se por exemplo as tecnologias de reconhecimento facial, já existem trabalhos demonstrando que minorias raciais e mulheres são especialmente afetadas por erros na aplicação desses sistemas. Taxas de falsos positivos de 40% para pessoas não-brancas e de 5% para pessoas brancas foram identificadas na ferramenta *Amazon Rekognition*, por exemplo (Whittaker *et al.*, 2018, p. 15-6).

Em uma outra pesquisa (Grother; Ngan; Hanaoka, 2019), realizada pelo *National Institute of Standards and Technology* (NIST) que avaliou e mediu as ocorrências de

falsos positivos e falsos negativos⁹ em 189 algoritmos de 99 desenvolvedores de reconhecimento facial diferentes, demonstrou que nos algoritmos norte-americanos ocorreram uma taxa mais alta de falsos positivos para rostos asiáticos, negros e indígenas em relação a pessoas brancas. Segundo esse estudo mulheres negras são o grupo mais atingido (Grother; Ngan; Hanaoka, 2019).

Por falsos negativos compreenda-se a situação em que o sistema não consegue encontrar a correspondência de um rosto à sua assinatura facial existente em um banco de dados, enquanto falsos positivos, por sua vez, dá-se justamente na situação oposta, ou seja, o sistema faz reconhecimento erroneamente, combinando um rosto com uma assinatura facial que não está presente no banco de dados (Konno Júnior.; Moura Jorge, 2023).

Pois bem, partindo-se da própria premissa do algoritmo de que os dados de um rosto humano fornecem informações apenas objetivas, não há, aparentemente qualquer razão que justifique a ocorrência da diferença estatística nos erros entre grupos étnicos ou gêneros diferentes e, se existem, fica claro que não passa de uma grande falácia o argumento de que uma máquina, por não ser dotada de emoções humanas, não é capaz de ter empatia ou preconceitos.

Vale ainda lembrar que a existência de vieses algorítmico acaba por violar princípios fundamentais insculpidos na Constituição Federal que proíbe o tratamento não igualitário ou discriminatório de qualquer natureza. O comando proibitivo é dirigido não apenas à população, mas principalmente ao próprio Estado, que fica impedido de adotar qualquer política pública capaz de violar essa garantia constitucional, aí se incluindo ferramentas e estratégias tecnológicas. Por via de consequência, ao uso de ferramentas baseadas em IA que tenham (ou potencialmente possam ter) padrões discriminatórios são constitucionalmente proibidos e, portanto, inaceitáveis.

A identificação desses vieses, no entanto, não é tarefa fácil e exige alto conhecimento especializado em diversas áreas do conhecimento. Em alguns casos, ele poderá ser até mesmo impossível de corrigir sem comprometimento da eficiência e da integridade do próprio sistema.

Isso se afirma porque existem inúmeras formas de discriminação que vão desde aquelas baseadas em dados eminentemente objetivos, como a geolocalização, até aquelas baseadas em dados subjetivos ou produzidos a partir de dados sensíveis sobre os cidadãos.

Quando o indivíduo é categorizado e julgado, por exemplo, a partir do grupo social a que pertence ou da área geográfica onde está inserido, pode-se facilmente mascarar

⁹ Um falso negativo significa que o sistema não foi capaz de identificar que duas fotos mostra a mesma pessoa enquanto que os falsos positivos as imagens de pessoas diferentes são interpretadas como sendo do mesmo indivíduo.

o viés discriminatório em suposta isenção baseada em dados estatísticos, assim como quando se utilizam dados de má qualidade, quando há falhas na metodologia empregada a discriminação pode se apresentar revestida de uma aura de critério científico que não correspondente à realidade.

Peguemos por exemplo a utilização de dados antigos sobre indivíduos. Fatos ocorridos há muito tempo, embora possam ser considerados verdadeiros, não correspondem mais à realidade das pessoas sobre os quais se referem. Caso as bases de dados não sejam periodicamente revistas e atualizadas, corre-se o risco estabelecer-se uma discriminação perpétua de pessoas. É imperioso que existam mecanismos para a desconsideração de informações ultrapassadas e que não fazem mais sentido, pois caso contrário criam-se estigmas cruéis e permanentes, trancafiando-as sujeitos numa classificação que não mais lhe diz respeito. Esse padrão é em tudo idêntico ao preconceito humano que não é alvo de reavaliação.

Conclui-se assim que a discriminação pode ter alto grau de sofisticação, como a exploração indevida das fragilidades e vulnerabilidades reais das pessoas em um momento singular e recortado de sua vida, impedindo a mesma de sair de algum ciclo perverso.

Um exemplo nesse sentido, embora não ligado à área de segurança pública, é o caso do Kyle Behm, aplicado estudante de uma conceituada instituição acadêmica dos EUA, que mesmo tendo excelentes notas e destacado desempenho acadêmico foi recusado sumariamente em processos seletivos por 05 (cinco) empresas que usavam o software *Kronos*, de gestão de pessoas, que entre outros fatores avalia a personalidade de candidatos à colocação laboral. Descobriu-se posteriormente que as eliminações se davam em razão de histórico de transtorno mental havido há vários anos, mas que serviam de base para a tecnologia¹⁰ para impedir sua colocação no mercado.

3.2 Hipervigilância e Privacidade

Outra preocupação bastante relevante diz respeito ao uso abusivo das tecnologias de vigilância pelos órgãos do Estado, descambando para o que pode representar graves violações de privacidade e autoritarismo, tais como perseguição e banimento de pessoas ou de grupos sociais.

Quando o Estado coloca toda a coletividade em uma situação de hipervigilância, seu uso passa a depender do humor e intenções do governante de ocasião, que pode fa-

¹⁰ Infelizmente, a história termina de forma trágica. Mantido no estigma de seu histórico de sua condição mental, Kyle Behm deu fim à própria vida, quando tinha apenas 29 anos de idade. Esses fatos foram referido no documentário chamado “Persona: The Dark Truth Behind Personality Tests”, bem como no livro “*Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*”, Disponível na plataforma de streaming HBO Max.

cilmente usar de seus aparatos para perseguir e estigmatizar pessoas, classificando-as como potenciais delinquentes, ou mesmo promovendo o que a doutrina vem denominando como “autoritarismo digital”, criando-se regimes de repressão e manipulação da sociedade.

O ponto central da preocupação reside no receio de que o uso massivo de tecnologia na coleta, compartilhamento e tratamento de dados pelo Estado possa ocasionar um controle estatal de tamanha magnitude capaz de transformar em realidade a figura do “Grande Irmão” idealizada por George Orwell em sua obra 1984.

Vale lembrar que os princípios que regem a Administração Pública, estabelecidos pelo art. 37 da Constituição de 1988 exigem que qualquer ato administrativo seja específico e fundamentado, sob pena de nulidade. Nesse cenário a utilização de informações dos cidadãos pelo Poder Público, quando feita de forma massiva e indiscriminada, ofende não apenas os direitos fundamentais previstos no texto Magno, mas também regras ligadas à gestão administrativa.

O uso de sistemas de reconhecimento facial e de vigilância em tempo real levantam preocupações quanto à privacidade dos cidadãos, pois o uso indiscriminado de tecnologias pelo Estado não raro adentra na esfera da intimidade e vida privada, monitorando comportamentos, preferências, hábitos e outras individualidades constitucionalmente protegidas.

No Brasil a proteção de dados pessoais é garantida pela Lei 13.709/18 que trata da Proteção de Dados Pessoais (LGPD) que logo em seu início anuncia que seu objetivo é o de oferecer proteção aos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade, quanto ao tratamento de dados pessoais, inclusive nos meios digitais, por qualquer pessoa natural ou por pessoa jurídica de direito público ou privado.

A LGPD tem 65 artigos, distribuídos em 10 capítulos e foi inspirado em linhas específicas da regulação europeia como o Regulamento Geral de Proteção de Dados¹¹. Estão abrangidos pela proteção da norma todos e quaisquer dados, desde aqueles usados na qualificação civil (nome, endereço, e-mail, idade, estado civil e situação patrimonial, etc.), aos que caracterizam os cidadãos em sua individualidade como etnia, características antromórficas, dados médicos e correlatos. Também protege os dados comportamentais sensíveis como orientação sexual, credo, preferência política, padrões de consumo, etc. e, como parece óbvio, os dados relacionados com a trajetória de vida como registros de históricos escolares, profissionais, judiciais, associativos, entre outros.¹²

11 GDPR, em sua sigla em inglês.

12 O art. 5º da LGPD considera dados pessoais “sensíveis” aqueles relacionados à origem racial ou étnica, à convicção religiosa, à opinião política, à filiação a sindicato ou à organização de caráter religioso, filosófico ou político, bem como

Sejam eles obtido em qualquer tipo de suporte (papel, eletrônico, informático, som e imagem, etc.), tais dados são pessoais e seu uso é regulado para todos os fins e a nova lei não deixa margens para dúvidas, o verdadeiro proprietário do dado não é aquele que o utiliza, tampouco quem mantém em bancos de dados mas os seus detentores.

Assim, se o dado pessoal pertence estritamente à pessoa a quem ele diz respeito, sua utilização requer do consentimento dos titulares e embora isso pareça algo óbvio, as utilizações práticas demonstram uma zona cinzenta, principalmente quando quem se utiliza desses dados é o Poder Público. Quando informações particulares estão sendo coletadas e tratadas pelos órgãos de Estado sem que seu dono sequer tome conhecimento dessa atuação e de seus usos (que podem até mesmo serem usado contra os seus titulares), estamos diante de uma situação ilegal e proibida pelo ordenamento jurídico.

Isso ocorre, por exemplo, em sistemas de reconhecimento facial utilizados em blitz móveis, locais fixos e até mesmo nos uniformes de policiais sem que a população seja advertida de tais coletas. Para muitos autores isso representa uma forma de violação de direitos civis por ser a vigilância demasiadamente intrusiva sobre a privacidade dos indivíduos (Fussey; Murray, 2019, p. 19-20).

A preocupação decorrente do uso abusivo da vigilância estatal se materializa, principalmente, pelo fato de ocorrer uma extração generalizada e indiscriminada de dados dos indivíduos no espaço de convívio urbano, que acabam, por conseguinte, alterando as relações sociais e colocando, em última análise, todos os que são analisados na condição de potenciais suspeitos (Rodotà, 2004, p.99).

Em setembro de 2022 o Supremo Tribunal Federal (STF) enfrentou a questão acima, tendo então declarado que o compartilhamento de dados entre órgãos públicos deve ser restrito ao mínimo necessário à finalidade informada e está forçosamente obrigada a seguir critérios rígidos para atender às exigências da LGPD.¹³

Em outra decisão, essa de fevereiro de 2024, a 2ª Turma do Suprema Corte decidiu que provas obtidas sem autorização judicial a partir de dados preservados em contas da internet são nulas e não podem ser usadas em investigação criminal.¹⁴

3.3 Dependência Tecnológica

Outro fator constantemente apontado como prejudicial na implementação de IA

dados referentes à saúde ou à vida sexual, dados genéticos ou biométricos vinculados a uma pessoa natural.

13 A STF decisão foi tomada na ADI 6649 ajuizada pelo Conselho Federal da OAB e na ADPF 695 requerida pelo Partido Socialista Brasileiro e considerou também que devem ser realizado o controle de acesso aos dados, com fixação da responsabilidade civil dos servidores por uso indevido e a segurança no tratamento e na guarda de informações cadastrais dos cidadãos.

14 Habeas Corpus 222141 movido por Raquel Amaral Cardoso, pessoa investigada sobre irregularidades no Departamento Estadual de Trânsito (Detran) do Paraná.

na segurança pública diz respeito à progressiva dependência dos agentes de Estado aos sistemas automatizados, principalmente quando se dá o seu uso excessivo, como acima exemplificado.

A completa dependência da IA é um caminho a ser evitado, uma vez que pode tornar a sociedade vulnerável a falhas técnicas, ataques cibernéticos e interrupções no fornecimento de serviços essenciais sem que seja possível encontrar uma resposta efetiva.

Sistemas tecnológicos exigem investimentos contínuos em infraestrutura e capacitação dos profissionais de segurança e a burocracia estatal nem sempre permite que essas ações sejam adotadas com a frequência ou com a intensidade que realmente precisam. Assim, a falta de manutenção de equipamentos, a demora na atualização de programas ou de capacitação dos agentes que o executam podem comprometer a segurança pública, ampliando a margem para erros de utilização.

Além disso, em que pese todo o avanço tecnológico que agora experimentamos, pode-se afirmar que ainda não se fez possível a substituição de habilidades humanas irreplicáveis como a empatia, a intuição, a criatividade, o julgamento moral ou ético.

As máquinas ainda tomam suas decisões com base nas informações que lhes são inseridas, geralmente lógicas, objetivas e cartesianas, mas existem nuances da psique humana que tornam os indivíduos seres completamente únicos e irrepetíveis. Padrões emocionais, morais e até mesmo as idiosincrasias definem a individualidade das pessoas em bilhões de variantes que nem sempre podem ser categorizadas. Não seria piegas se recorrer à surrada expressão de que todo ser humano é único. Todas essas singularidades pesam na tomada de decisão dos indivíduos e são quase (senão completamente) impossíveis de replicar ou substituir por padrões baseados em IA.

Outro grande problema do uso da tecnologia é que apesar de sua crescente expansão, seu domínio ainda está nas mãos de poucas empresas ou governos. É necessário criar mecanismos para democratizar a IA e os conhecimentos dela advindos para evitar o monopólio pois somente o poder do conhecimento aberto nos permitirá compreender melhor os riscos e as formas de defesa contra ameaças tecnológicas.

Obviamente, esses não são os únicos desafios da implementação de IA no Setor Público, Vasconcelos & Santos (2024) discorrem sobre os problemas que vão desde a infraestrutura até a capacitação dos operadores, destacando, assim como o fazemos nesse artigo, os sérios problemas relacionados à ética e privacidade.

4 DISCUSSÃO E ESTRATÉGIAS

Feitas todas essas ponderações sobre uso da IA na segurança pública, é preciso definir se as vantagens e benefícios superam, em numa relação de custo-benefício os

riscos e desafios envolvidos, ou ainda se é possível evitar-se os potenciais danos que já se vislumbram.

A otimização e a eficiência proporcionadas pela tecnologia são evidentes, mas devem ser ponderadas com os riscos éticos e sociais. Em países como os Estados Unidos e China, o uso da IA em segurança pública já demonstrou resultados significativos em termos de eficiência, mas também levantou polêmicas e levou a discussões sobre a regulamentação do uso dessas tecnologias.

O que nos parece evidente é que é crucial desenvolver políticas públicas que estabeleçam diretrizes claras sobre o uso de IA, respeitando tanto os benefícios que ela pode oferecer quanto a proteção dos direitos fundamentais dos cidadãos. Além disso, é importante investir em transparência e supervisão para mitigar os riscos de discriminação e uso indevido de dados pessoais.

Para que isso aconteça, se faz necessário estabelecer regras claras e rígidas de uso dessa tecnologia, o que, felizmente, já vem sendo debatido por pesquisadores, desenvolvedores e pelo Ministério da Ciência, Tecnologia e Inovação (MCTI).

No Brasil foi criada recentemente a Estratégia Brasileira de Inteligência Artificial (EBIA) para pensar os rumos, propor regulações e aperfeiçoamento dessa tecnologia.

Em publicação produzida em 2021, a EBIA traçou algumas providências para o uso de tecnologias de IA no contexto de segurança pública, com o escopo de assegurar maior respeito aos direitos de privacidade e de proteção de dados pessoais em conformidade com os direitos constitucionais à intimidade, à privacidade e à proteção à imagem do titular. Defendeu-se ali que a criação e o uso de bancos de dados de segurança pública integrado aos sistemas de IA devem observar o devido processo legal, os princípios gerais de proteção de dados pessoais e os direitos dos titulares de dados, conforme o art. 4º, §1º, da LGPD.

Submetida ao debate público em 2021, foram elencadas algumas medidas entendidas como necessárias pelo EBIA para o uso adequado da IA na Segurança Pública que em apertada síntese discurremos abaixo.

Compreendeu-se necessária a adoção de mecanismos de *soft law*, com a produção de guias e recomendações que auxiliem reguladores e regulados a aplicar as previsões normativas das leis relevantes a exemplo do que ocorreu nas experiências européias produziram relatórios analíticos quanto ao uso de reconhecimento facial em espaços públicos pela polícia¹⁵ e quanto ao uso de câmeras de vigilância, com uma seção dedicada a sistemas inteligentes¹⁶, assim como a adoção de um programa de aprimoramento desses sistemas, como fizeram os EUA¹⁷.

15 Relatório publicado pela Information Commissioner's Office (ICO), do Reino Unido em 2019.

16 Relatório da European Data Protection Supervisor, de 2020.

17 Programa desenvolvido pelo National Institute of Standards and Technology – NIST.

Também defendeu-se a criação de estrutura de supervisão (*oversight*) com um ou mais representantes legitimados dotados de capacidade garantir a aplicabilidade da lei (*enforcement*) e com autoridade independente, para fins de monitoramento do uso das tecnologias em questão e adoção de remédios jurídicos eficazes para endereçar eventuais abusos.

Outra diretriz reside na adoção de normas ou padrões técnicos (*standardisation*) estabelecidos pelas comunidades técnico-científicas para orientar a indústria no desenvolvimento e implementação de soluções tecnológicas. Uma organização internacionalmente reconhecida pela publicação de padrões é a *International Organization for Standardization* (ISO) que no contexto de IA para segurança pública.¹⁸

Considerou-se urgente o estabelecimento de novas regulações de proteção de dados aplicadas à segurança pública já que o tratamento de dados em contexto de segurança pública necessita de lei específica, uma vez que este tema foge ao escopo da LGPD, lembrando que o próprio art. 4º, §1º daquela norma estabeleceu que o devido processo legal, os princípios gerais de proteção de dados pessoais e os direitos do titular de dados ali previstos devem estar presentes na lei específica a ser elaborada. Enquanto uma lei específica sobre o tema não existe, aplica-se a LGPD ainda que de forma limitada.¹⁹

Implementação de *sandbox* regulatório no ordenamento jurídico nacional, assim entendida como técnica regulatória que permite transparência a respeito de soluções tecnológicas desenvolvidas por entes privados ou estatais também foi destacada no documento. Em um *sandbox*, autoridades reguladoras de um determinado setor abrem editais públicos para que entidades se candidatem para construir testagens de soluções tecnológicas sob supervisão estatal. Isto permitirá um monitoramento contínuo da tecnologia que vem sendo desenvolvida identificando eventuais riscos. Desde que os avaliados obedeçam determinados parâmetros mínimos de segurança para a solução pretendida, permite-se ao regulador decidir se a tecnologia poderá ou não ser distribuída no mercado.

Avaliando cada uma dessas estratégias sugeridas, resta evidente que desde que o Estado brasileiro tenha esses instrumentos norteadores corretamente estabelecidos no desenvolvimento e na utilização da tecnologia, pode-se perfeitamente promover o avanço científico e solucionar problemas concretos do País em Inteligência Artificial, bem como seu uso consciente e ético no mundo e no Brasil.

18 Normas ISO que mereceram destaque foram a ISO/IEC 27001 e ISO/IEC 27701 pertinentes respectivamente aos sistemas de gestão da segurança e privacidade da informação e a ISO/IEC 37122 que trata de indicadores para cidades inteligentes (seção 15: segurança pública).

19 Tramita na Câmara dos Deputados Projeto de Lei 1515/22 trata da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPD) para fins de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais. A proposta tem o objetivo de regular artigo da LGPD que prevê regra específica para tratamento de dados pessoais nestes casos. Fonte: Agência Câmara de Notícias.

5 CONCLUSÕES

A inteligência artificial tem o potencial de transformar a segurança pública, oferecendo ferramentas que podem aumentar a eficácia e a eficiência das forças de segurança e embora seu uso ainda apresente riscos, considerando as implicações éticas e sociais envolvidas. Seu uso cauteloso traz vantagens que em muito superam os problemas pontuais na utilização.

É fundamental que o Brasil desenvolva uma regulamentação robusta capaz de garantir a utilização responsável da IA, priorizando a proteção dos direitos dos indivíduos, respeitando o direitos fundamentais, eliminando os casos de discriminação ou de potenciais violações de privacidade que venham a ser detectados.

As atuais diretrizes sugeridas pela Estratégia Brasileira de Inteligência Artificial (EBIA) e as diversas iniciativas de estudo da IA apontam caminhos importantes não só para orientar as futuras regulações, como para o desenvolvimento das futuras tecnologias, mas o debate deve permanecer ininterrupto, face a velocidade com que a realidade se altera.

Desde que adotadas essas cautelas é possível aproveitar plenamente os benefícios da IA na segurança pública para que se estabeleça como uma tecnologia que possa contribuir para gerar riquezas, melhorar a qualidade de vida dos indivíduos e garantir os direitos fundamentais de todos.

ADVANTAGES AND RISKS INVOLVED IN THE USE OF ARTIFICIAL INTELLIGENCE IN PUBLIC SAFETY

ABSTRACT

This article analyzes the advantages and risks involved in using artificial intelligence in public security, particularly its practical application by state security agencies. While there are evident benefits to its use, such as resource optimization, agility in data processing, and the ability to identify criminal patterns, there are also risks and concerns related to ethical issues, the presence of biases in algorithms, and threats to citizens' privacy. Through a literature review and analysis of ongoing practical experiences, it was concluded that, despite the challenges, with responsible and regulated use, AI technology can positively contribute to the efficiency of public security.

Keywords: artificial intelligence; public security; advantages; disadvantages; bias; privacy.

REFERÊNCIAS

BADAL, Murilo Maffioletti; OLIVEIRA, Marlo. **Inteligência artificial na segurança pública**: o uso do reconhecimento facial para identificação de infratores. Repositório Eletrônico de artigos da Universidade Extremo Sul Catarinense - UNESC. Criciúma. 2024 Disponível em: <http://repositorio.unesc.net/bitstream/1/10986/1/Murilo%20Maffioletti%20Bada.pdf>. Acesso em: 24 nov. 2024.

BIGATON, Tainá Rafaela; TEIXEIRA, Marcelo Markus; BILHALVA, João Vítor Massaro. A ética de dados como uma possível resposta para alguns desafios do direito internacional frente a inteligência artificial. **Revista Eletrônica do Curso de Direito da UFSM**, V. 17, n. 1. Chapecó 2022. Disponível em : <https://periodicos.ufsm.br/revistadireito/article/download/65051/51512/357271>. Acesso em: 20 nov. 2024.

BRASIL. **Lei nº 13.709 de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://bit.ly/2GrnTML>. Acesso em: 22 nov. 2024.

BRASIL. **Projeto de Lei 1515/2022**. Dispõe sobre a Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Congresso Nacional. 07 jun. 2022. Disponível em: <https://www.congressonacional.leg.br/materias/materias-bicamerais/-/ver/pl-1515-2022>. Acesso em: 23 nov. 2024.

BRASIL. Estratégia Brasileira de Inteligência Artificial. Ministério da Ciência, Tecnologia e Inovações - MCTI. Brasília, 2021. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf. Acesso em: 20 nov. 2024.

CORVALÁN, Juan. Inteligencia artificial: retos, desafíos y oportunidades. Prometea: la primera inteligencia artificial de Latinoamérica al servicio de la Justicia. **Revista de Investigaciones Constitucionales**, v. 5, n. 1, 2017.

FUSSEY, Pete; MURRAY, Daragh. Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology. The Human Rights, Big Data and Technology Project - Human Rights Center, University of Essex, 2019. Disponível em: <https://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf>. Acesso em: 06 nov. 2024.

GOVERNO DO CEARÁ. Ações das Forças da SSPDS resultam no aumento de 24,8% nas capturas por furto e receptação de fios em Fortaleza em 2024. Fortaleza, 20 set. 2024. Disponível em: <https://www.sspds.ce.gov.br/2024/09/20/acoes-das-forcas-da-sspds-resultam-no-aumento-de-248-nas-capturas-por-furto-e-receptacao-de-fios-em-fortaleza-em-2024/>. Acesso em: 24 nov. 2024.

GOVERNO DO CEARÁ. Com integração de informações e base de dados, Agilis é lançado pela SSPDS como mais uma ferramenta de inteligência no combate ao crime. Fortaleza, 20 maio 2021. Disponível em: <https://www.sspds.ce.gov.br/2021/05/20/com-integracao-de-informacoes-e-base-de-dados-agilis-e-lancado-pela-sspds-como-mais-uma-ferramenta-de-inteligencia-no-combate-ao-crime/>. Acesso em: 24 nov. 2024.

GLESS, Sabine. Policiamento preditivo: em defesa dos “verdadeiros positivos”. Tradução Heloisa Estellita e Miguel Lima Carneiro. **Revista de Direito da Fundação Getúlio Vargas**. V. 16, n. 1, São Paulo 2020. Disponível em: https://bdjur.stj.jus.br/jspui/bitstream/2011/143830/policiamento_preditivo_defesa_gless.pdf. Acesso em: 23 nov. 2024.

GONÇALVES, Mariana Sbaite. Viés algorítmico e discriminação: Como os algoritmos de IA podem perpetuar e amplificar vieses sociais. **Revista Migalhas**, 12 set. 2024. Disponível em: <https://www.migalhas.com.br/depeso/415125/vies-algoritmico-e-discriminacao-ia-pode-amplificar-vieses-sociais>. Acesso em: 20 nov. 2024.

HARTMANN Ivar Alberto Martins; FRANQUEIRA Bruna; UNES Julia, ABBAS, Lorena; CURZI Yasmin, VILLA Beatriz; ABREU Fernanda, DIAS Renan. Policy Paper: Regulação de Inteligência Artificial no Brasil. Fundação Getúlio Vargas. Rio de Janeiro 2020. Disponível em: <https://diretorio.fgv.br/conhecimento/policy-paper-regulacao-de-inteligencia-artificial-no-brasil>. Acesso em: 23 nov. 2024.

KONNO JÚNIOR, J.; MOURA JORGE, D. Inteligência Artificial no reconhecimento facial em Segurança Pública: dados sensíveis e seletividade penal. **Direito & TI**, [S. l.], v. 1, n. 15, p. 61–80, 2023. DOI: 10.63451/ti.v1i15.123. Disponível em: <https://www.direitoeti.com.br/direitoeti/article/view/123>. Acesso em: 30 maio 2025.

LUNA, Carlos Rogério Pereira. Uso da inteligência artificial como ferramenta auxiliar na atividade policial de inteligência de segurança pública. **Revista ft TH Ciências Exatas e da Terra**, vol. 28 edição 134, maio 2024.

MELO, R. A.; SILVA, T. Desafios éticos no uso de IA em segurança pública no Brasil. **Revista de Direito e Tecnologia**, vol. 5, no. 1, pp. 55-67, 2022.

MELLO, Breno César de Souza. Discriminação algorítmica, vigilância eletrônica e questões de segurança. **Revista Eletrônica Consultor Jurídico**, 07 mar. 2024. Disponível em: <https://www.conjur.com.br/2023-mar-07/souza-mello-discriminacao-algoritima-vigilancia-eletronica/>. Acesso em: 13 nov. 2024.

MENDES, Laura; MATTIUZZO, Marcela. Proteção de dados e inteligência artificial: perspectivas éticas e regulatórias. **RDU**, Porto Alegre, Volume 16, nº 90, 2019, 39-64, nov-dez 2019.

MENDONÇA, Jean Michel Barbosa; SILVA, Adelino Pinheiro. O Viés de confirmação Pericial: Casos em Exames Periciais Comparativos e Possíveis Medidas de Contenção. **Revista Acadêmica Avante**, Belo Horizonte, v.1 - n.5 I 2023 jul.-dez. 2023.

NAGATA, Sabrina Vettorazzi. Utilização da inteligência artificial na segurança pública e sua contribuição na Polícia Militar. **Brazilian Journal of Development**, Curitiba, v.10, n.6, p. 01-18, 2024.

NICKERSON, Raymond. Confirmation bias: A ubiquitous phenomenon in many guises. **Review of general psychology**, v. 2, n. 2, p. 175-220, 1998.

O'NEIL, Cathy. **Weapons od Math Destruction: How Big Data Increases Inequality and Threatens Democracy**. Nova York: Crow Publishig, 2016.

ORWELL, George. **1984**. São Paulo: Companhia das Letras, 2009.

PERSONA: The Dark Truth Behind Personality Tests. Documentário. Direção Tim Travers Hawkins. 2021 (1h e 25 m) Disponível na Prime Vídeo.

RODOTÀ, Stefano. **A vida na sociedade da vigilância – A privacidade hoje**. Organização seleção e apresentação de Maria Celina Bodin de Moraes, tradução de Danilo Doneda e Luciana Cabral Doneta Rio de Janeiro; Renovar. 2008.

SALES, E. R. de; LUI, L. Perspectivas sobre segurança pública em cidades inteligentes: uma revisão da literatura de 2002 a 2022. **Revista de Gestão dos Países de Língua Portuguesa**, Rio de Janeiro, v. 22, n. 2, p. 83–101, 2023. DOI: 10.12660/rgplp.v22n2.2023.88882. Disponível em: <https://periodicos.fgv.br/rgplp/article/view/88882>. Acesso em: 30 maio 2025.

SANTOS, Reginaldo Angelo dos; SARKIS, Sadik; DAMAS Déborah Alessandra de Oliveira; BISTENE, Luisa França. LGPD – Vigilância Estatal ou direito à privacidade de dados. **Revista Migalhas**, 16 de dezembro de 2022. Disponível em: <https://www.migalhas.com.br/depeso/378590/lgpd—vigilancia-estatal-ou-direito-a-privacidade-de-dados>. Acesso em: 23 nov. 2024.

SELA, Vilma Meurer; SOARES, Augusto Cesare de Campos. Os desafios da administração pública na era do conhecimento e da informação. **Universidade Estadual de Maringá**. Maringá 2014. v. 22, n. 1. Acesso em: 11 nov. 2024. Disponível em: <https://periodicos.uem.br/ojs/index.php/CadAdm/article/download/23122/16047/>. Acesso em: 04 nov. 2024.

SILVA, Denis William da. **Tecnologia da Informação Aplicada à Vigilância com Reconhecimento Facial e Inteligência Artificial**. 2023. Dissertação de Mestrado apresentado à escola de administração de empresas de São Paulo da Fundação Getúlio Vargas. São Paulo, 2023.

SOUZA, L.; MENDONÇA, A. M. A Lei Geral de Proteção de Dados e a segurança pública. **Revista Jurídica da Universidade Federal do Paraná**, Curitiba, vol. 7, no. 3, pp. 112-125, 2020.

STF e proteção de dados pessoais: decisões da Corte marcaram a evolução de um novo direito fundamental. **Supremo Tribunal Federal**. Brasília 14 ago.2024. Disponível em: <https://noticias.stf.jus.br/postsnoticias/stf-e-protecao-de-dados-pessoais-decisoes-da-corte-marcaram-a-evolucao-de-um-novo-direito-fundamental/>. Acesso em: 22 nov. 24.

TELLES, Primonata Silva Brilhante. Inteligência artificial e polícia preditiva: limites e possibilidades. **Boletim Científico ESMPU**, Brasília, a. 20, n. 57, jul./dez. 2021. Disponível em: <https://escola.mpu.mp.br/publicacoesscientificas/index.php/boletim/article/view/613>. Acesso em: 20 nov. 2024.

VASCONCELOS, E. S., & SANTOS, F. A. dos. (2024). Inteligência artificial na gestão pública brasileira: desafios e oportunidades para a eficiência governamental. *Observatório de La Economia Lationoamericana*, 22(6), e5017. Disponível em: <https://doi.org/10.55905/oelv22n6-020>. Acesso em: 03 jun. 2025.