

**INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE
GOIÁS CAMPUS INHUMAS
SISTEMAS DE
INFORMAÇÃO**

JEAN CARLOS L. VIEIRA

**PEDRO BORGES F.
SALVATO**

**UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA:
UMA REVISÃO BIBLIOGRÁFICA**

INHUMAS

2023

JEAN CARLOS LÚCIO VIEIRA

PEDRO BORGES F.
SALVATO

UTILIZAÇÃO DE INTELIGÊNCIA ARTIFICIAL NA SEGURANÇA PÚBLICA:
UMA REVISÃO BIBLIOGRÁFICA

Trabalho de Conclusão de Curso apresentado ao curso de Sistemas de Informação, do Instituto Federal de Educação, Ciência e Tecnologia de Goiás - Campus Inhumas/IFG, como requisito parcial à obtenção do título de Bacharel em Sistemas de informação

Orientador(a): Prof(a). Mr(a). Ricardo Rodrigues Dias de Lima

INHUMAS
2023

TERMO DE AUTORIZAÇÃO PARA DISPONIBILIZAÇÃO
NO REPOSITÓRIO DIGITAL DO IFG - ReDi IFG

Com base no disposto na Lei Federal nº 9.610/98, AUTORIZO o Instituto Federal de Educação, Ciência e Tecnologia de Goiás, a disponibilizar gratuitamente o documento no Repositório Digital (ReDi IFG), sem ressarcimento de direitos autorais, conforme permissão assinada abaixo, em formato digital para fins de leitura, download e impressão, a título de divulgação da produção técnico-científica no IFG.

Identificação da Produção Técnico-Científica

- | | |
|--|---|
| ☐ Tese | ☐ Artigo Científico |
| ☐ Dissertação | ☐ Capítulo de Livro |
| ☐ Monografia – Especialização | ☐ Livro |
| ☒ TCC - Graduação | ☐ Trabalho Apresentado em Evento |
| ☐ Produto Técnico e Educacional - Tipo: _____ | |

Nome Completo do Autor: Jean Carlos Lúcio Vieira

Matrícula: 20201030090130

Nome Completo do Autor: Pedro Borges Fernandes Salvato

Matrícula: 20201030090148

Título do Trabalho: Utilização de IA na segurança pública: Uma revisão bibliográfica

Autorização - Marque uma das opções

1. ☒ Autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso aberto);
2. ☐ Autorizo disponibilizar meu trabalho no Repositório Digital do IFG somente após a data ____/____/____(Embargo);
3. ☐ Não autorizo disponibilizar meu trabalho no Repositório Digital do IFG (acesso restrito).

Ao indicar a opção **2 ou 3**, marque a justificativa:

☐ O documento está sujeito a registro de patente.

☐ O documento pode vir a ser publicado como livro, capítulo de livro ou artigo.

☐ Outra justificativa: _____

DECLARAÇÃO DE DISTRIBUIÇÃO NÃO-EXCLUSIVA

O/A referido/a autor/a declara que:

- i. o documento é seu trabalho original, detém os direitos autorais da produção técnico-científica e não infringe os direitos de qualquer outra pessoa ou entidade;
- ii. obteve autorização de quaisquer materiais inclusos no documento do qual não detém os direitos de autor/a, para conceder ao Instituto Federal de Educação, Ciência e Tecnologia de Goiás os direitos requeridos e que este material cujos direitos autorais são de terceiros, estão claramente identificados e reconhecidos no texto ou conteúdo do documento entregue;
- iii. cumpriu quaisquer obrigações exigidas por contrato ou acordo, caso o documento entregue seja baseado em trabalho financiado ou apoiado por outra instituição que não o Instituto Federal de Educação, Ciência e Tecnologia de Goiás.

Inhumas, 15 de Fevereiro de 2024.

Local

Data

Assinatura do Autor e/ou Detentor dos Direitos Autorais

Dados Internacionais de Catalogação na Publicação

Vieira, Jean Carlos Lúcio.

V658 Utilização de Inteligência Artificial na Segurança Pública: uma revisão bibliográfica [Manuscrito]. / Jean Carlos Lúcio Vieira, Pedro Borges Fernandes Salvato. – Inhumas: IFG, 2023.

64 f. : il.

Inclui bibliografia.

Orientador: Prof. Me. Ricardo Rodrigues Dias de Lima.

Trabalho de Conclusão de Curso Bacharelado em Sistemas de Informação – IFG/Câmpus Inhumas, 2023.

1. Inteligência artificial. 2. Revisão bibliográfica. 3. Segurança pública. I. Salvato, Pedro Borges Fernandes. II. Lima, Ricardo Rodrigues Dias de (Orient.). III. Título.

CDD 006.3

Ficha catalográfica elaborada pela bibliotecária
Maria Aparecida Rodrigues de Souza - CRB/1-1497
Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Câmpus Inhumas – Biblioteca Atena



INSTITUTO FEDERAL
Goiás

MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE GOIÁS
CÂMPUS INHUMAS

ATA DA SESSÃO PÚBLICA DE APRESENTAÇÃO E DEFESA DO TRABALHO DE CONCLUSÃO DE CURSO

Aos 14 (quatorze) dias do mês de dezembro do ano de 2023, às 21 horas, compareceram perante a banca examinadora os alunos **Jean Carlos Lúcio Vieira** e **Pedro Borges Fernandes Salvato** autores do Trabalho de Conclusão de Curso intitulado **Utilização de Inteligência Artificial na Segurança Pública: uma revisão bibliográfica**, sendo a banca examinadora constituída pelos professores Ricardo Rodrigues Dias de Lima (orientador), Cleiton José da Silva (1º examinador) e Rodrigo Cândido Borges (2º examinador) que atribuíram, respectivamente, as seguintes notas: (8,0), (8,0), (8,0), cuja média aritmética é 8,0 (oito pontos), tendo a referida banca considerado os alunos aprovados e aptos para a Colação de Grau de **Bacharel em Sistemas de Informação**.

E por estar conforme, eu Ricardo Rodrigues Dias de Lima, lavrei a presente ata que vai assinada por mim, pelos membros da banca e pelo coordenador do curso de Bacharelado em Sistemas de Informação.

Orientador(a): Ricardo Rodrigues Dias de Lima

1º examinador(a): Cleiton José da Silva

2º examinador(a): Rodrigo Cândido Borges

Coordenador do curso de Bacharelado em Sistemas de Informação: Rodrigo Cândido Borges

Documento assinado eletronicamente por:

- **Rodrigo Candido Borges**, COORDENADOR(A) DE CURSO - FUC1 - INH-CCBES, em 16/12/2023 19:20:31.
- **Cleiton Jose da Silva**, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 16/12/2023 08:38:58.
- **Ricardo Rodrigues Dias de Lima**, PROFESSOR ENS BASICO TECN TECNOLOGICO, em 15/12/2023 19:07:52.

Este documento foi emitido pelo SUAP em 15/12/2023. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse <https://suap.ifg.edu.br/autenticar-documento/> e forneça os dados abaixo:

Código Verificador: 491407

Código de Autenticação: 31c5da3c6e



Instituto Federal de Educação, Ciência e Tecnologia de Goiás
Av. Universitária, S/Nº, Vale das Goiabeiras, INHUMAS / GO, CEP 75402-556
(62) 3514-9557 (ramal: 9557)

RESUMO

A utilização da Inteligência Artificial (IA) tem se tornado popular na atualidade, e sua aplicação pode ser observada em diferentes escopos, destacando-se a área da segurança pública, cujas aplicações abrangem desde uso domiciliar até aplicações governamentais e militares. Devido à essa popularização, os benefícios e as problemáticas que a circundam são evidenciadas, gerando assim discussões acerca de sua utilização. O objetivo desta revisão de literatura é realizar um levantamento de dados sobre o assunto, buscando compreender o estado da arte atual da pesquisa sobre o tema. Além disso, também foi buscado entender, pontuar e discutir as principais problemáticas e implicações éticas acerca da utilização de Inteligência Artificial na Segurança Pública. Dessa maneira, o material foi coletado, comparado e selecionado a fim de tornar a pesquisa mais completa e precisa.

Palavras chave: Inteligência artificial, Segurança pública, revisão de literatura

ABSTRACT

The use of Artificial Intelligence (AI) has become popular nowadays, and its application can be observed in different scopes, particularly in the field of public security, where applications range from household use to governmental and military applications. Due to this popularization, the benefits and issues surrounding it are highlighted, thus generating discussions about its usage. The objective of this literature review is to gather data on the subject, seeking to understand the current state of the art of research on the topic. Additionally, it also aimed to understand, point out, and discuss the main issues and ethical implications regarding the use of Artificial Intelligence in Public Security. In this way, the material was collected, compared, and selected to make the research more comprehensive and accurate.

Keywords: Artificial Intelligence, Public security, Literary review

LISTA DE FIGURAS

Figura 1: Taxa de pesquisa do termo “inteligência artificial” de 01/01/22 a 15/07/2023. Fonte: Google trends

Figura 2: Taxa de pesquisa do termo “ChatGPT” de 01/01/22 a 15/07/2023. Fonte: GOOGLE TRENDS.

Figura 3: Recorte da visão geral dos estudos incluídos em nossa revisão sistemática da literatura. Fonte: ZUIDERWIJK, 2021

Figura 4: Recorte de benefícios em potencial do uso de IA no governo, identificados nos estudos exemplificados. Fonte: ZUIDERWIJK, 2021

Figura 5: Principais aplicações identificadas. Fonte: Autores(2023).

Figura 6: Quantidade de trabalhos por string. Fonte: Autores(2023)

Figura 7: Comparação dos resultados. Fonte: Fonte: Xiaoying Qiu(2019)

LISTA DE QUADROS

Quadro 1 - Strings de busca. Fonte: Autores(2023)

Quadro 2 - Strings utilizadas para obtenção da quantidade total de trabalhos. Fonte: Autores(2023)

Quadro 3 - Critérios de inclusão e exclusão de trabalhos. Fonte: Autores(2023)

Quadro 4 - Listagem dos trabalhos encontrados, mostrando qual o tema e também as principais técnicas utilizadas(quando houver). Fonte: Autores(2023)

LISTA DE ABREVIATURAS OU SIGLAS

CCTV	Closed-circuit television(Circuito fechado de televisão)
CLN	Compreensão da linguagem natural
EUA	Estados Unidos da América
GAN	Generative adversarial network (Rede Adversarial Generativa)
GLN	Geração de linguagem natural
IA	Inteligência artificial
IoT	Internet of things (internet das coisas)
LC	Literatura cinzenta
PLN	Processamento de linguagem natural
RB	Revisão bibliográfica
RLM	Revisão de literatura multivocal
RSL	Revisão sistemática de literatura
RTIC	Real-Time Intelligence Center(Centro de inteligência em tempo-real)
SP	Segurança pública
SRGANs	Super resolution generative adversarial network (Rede adversarial generativa de super resolução)
TCC	Trabalho de Conclusão de Curso
TIC	Tecnologias de Informação e Comunicação
TRF	Tecnologias de Reconhecimento Facial
UAV	Unidentified Aerial Vehicle(Veículo Aéreo não tripulado)
VANT	Veículo Aéreo não tripulado

SUMÁRIO

1. INTRODUÇÃO.....	13
1.1 Organização do trabalho.....	16
2. REFERENCIAL TEÓRICO.....	17
2.1.1 Inteligência artificial.....	17
2.1.2 ChatBOTS.....	18
2.1.3 Segurança pública.....	20
2.1.4 Segurança pública x Inteligência artificial.....	20
2.1.5 Racionalidade.....	22
2.1.6 Ética.....	23
2.1.7 Inteligência artificial e ética.....	23
2.1.8 Cidades inteligentes(smart cities).....	24
3. METODOLOGIA.....	25
4. PLANEJAMENTO DA REVISÃO.....	28
4.1 Revisão de literatura multivocal.....	28
4.1.1 Revisão Narrativa de literatura.....	28
4.1.2 Objetivos e questões de pesquisa.....	28
4.1.3 Strings de busca.....	29
4.1.4 Motores de busca.....	31
4.1.5 Critérios de inclusão, exclusão e qualidade.....	31
4.1.6 Métodos de seleção de trabalho.....	32
4.1.7 Análise dos trabalhos.....	32
4.1.8 Busca na Literatura Cinzenta.....	36
4.1.9 AI For Smart Policing.....	37
4.1.10 Using Chatbot Technology to Improve how Law Enforcement Responds to Victims of Residential Burglary.....	37
4.1.11 Artificial intelligence bolsters public safety & security in smart cities.....	38
5. RESULTADOS DA RLM.....	39
5.1. Busca do número total de trabalhos.....	45
6. DISCUSSÃO DOS PRINCIPAIS TERMOS E RESULTADOS.....	47
6.1 Smart policing.....	47
6.2 CCTV.....	48
6.3 Smart cities.....	49
6.4 Cyberattacks.....	50
6.5 Drone/UAV.....	52
6.6 Chatbot.....	52

6.7. A Ética nos trabalhos.....	53
7. CONCLUSÃO.....	56
REFERÊNCIAS.....	57

1. INTRODUÇÃO

Com a evolução da tecnologia, o tema da segurança pública(SP) vem se tornando cada vez mais relevante, bem como o uso de inteligência artificial (IA) nesse escopo. Há inúmeras aplicações da IA na SP, dentre as quais, pode-se citar: “Tecnologias de Reconhecimento Facial(TRF)” (FRA, 2019) e “melhoramento de imagens das câmeras de segurança por meio de upscaling (BERA, 2011)”.

A aplicação das IAs na segurança pública não é novidade, de fato, já tem sido utilizado por autoridades em diferentes locais no mundo. Contudo, muitas controvérsias cercam esses assuntos. Um exemplo clássico disso é a invasão de privacidade.

“O uso de tal sistema implica na monitorização contínua de espaços públicos e, conseqüentemente, na vigilância de atividades humanas e presenças, levantando preocupações urgentes sobre privacidade e potenciais ameaças aos direitos e liberdades individuais (FRA, 2019)”.

Em uma busca preliminar na base de trabalhos científicos Google Acadêmico, utilizando as palavras chave “SP” e “IA”, foram encontrados 2.860 trabalhos em língua portuguesa, utilizando como intervalo de tempo os anos 2020 - 2023. Nessas buscas, foram encontradas diversas revisões de literatura que trataram sobre a utilização de IA na governança pública e suas particularidades (administração, gestão, saúde, inovação e segurança). Contudo, foi identificada uma carência de revisões de literatura que tratam especificamente da utilização de IA na SP.

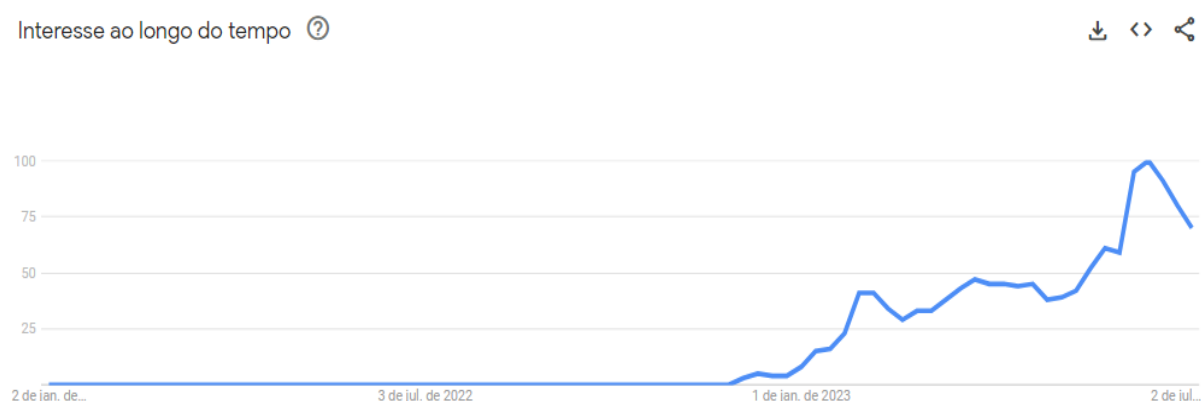
Figura 1: Taxa de pesquisa do termo “inteligência artificial” de 01/01/22 a 15/07/2023.



Fonte: Google Trends (2023).

Com base na Figura 1, é possível perceber um aumento exponencial no interesse pelas buscas sobre IA, principalmente no ano de 2023. Tal fato deve-se, principalmente, a popularização de uma forma específica de IA conhecida como *chatbot*, tendo como principal expoente o ChatGPT.

Figura 2 - Taxa de pesquisa do termo “ChatGPT” de 01/01/22 a 15/07/2023



Fonte: Google Trends (2023)

Conforme evidenciado nas Figuras 1 e 2, houve grande disseminação no interesse pelo tema, tornando-o mais acessível. A IA promete proporcionar benefícios significativos para empresas e a sociedade em geral, mas também tem o potencial de causar danos significativos se não compreendermos os riscos que essa

tecnologia apresenta (BROOM, 2023). Vale ressaltar que *chatbots* não são a única forma de aplicação de IAs na área. Entre os exemplos existentes destaca-se: tecnologias de reconhecimento facial, monitoramento à distância, entre outros.

O objetivo desta revisão é analisar, discutir e expor as vantagens e desvantagens, utilizações e possibilidades do uso de IAs no setor da SP, e também suas implicações éticas e sociais. Para o desenvolvimento do estudo, serão utilizados métodos de pesquisa rigorosos, incluindo revisão da literatura atualizada, exposição dos dados em tabelas, análise estatística adequada e interpretação dos resultados à luz da teoria existente.

A pesquisa sobre a utilização de IA na segurança pública possui grande relevância acadêmica. É uma área multidisciplinar que envolve conhecimentos de ciência da computação, direito, ciências sociais e outras áreas correlatas. Uma revisão bibliográfica sobre o assunto pode contribuir para o conhecimento científico acumulado, identificando as principais tendências, desafios e lacunas de pesquisa na área. Além disso, pode fornecer uma base teórica sólida para futuras pesquisas e projetos relacionados à utilização de IA na segurança pública, sendo uma contribuição valiosa para a academia e para profissionais interessados na área.

Por fim, a atualidade do tema também é um fator relevante. É difícil compreender o potencial a longo prazo da IA para mudar aspectos-chave da forma como vivemos e para apoiar o funcionamento de empresas, governos e outras organizações (BERGLIND; FADIA; ISHERWOOD, 2022). O autor Bertino (2021) também cita:

“[...]Também, abordagens de cibersegurança baseadas em IA têm sido intensamente examinadas em relação à ética. Portanto, para que a IA seja adotada de maneira eficaz e rápida na cibersegurança, a segurança e a ética da IA também precisam ser garantidas. A segurança da IA exige processos de garantia para os dados utilizados no treinamento da IA, assim como abordagens sistemáticas para testes de segurança da IA. Em relação à ética, precisamos desenvolver abordagens técnicas para incorporar princípios éticos em sistemas inteligentes.”

O objetivo geral do presente trabalho é realizar uma revisão bibliográfica narrativa multivocal sobre a utilização de Inteligência Artificial na segurança pública, que busca compreender o estado da arte da pesquisa sobre o tema. Para alcançar

esse objetivo, foram também definidos cinco objetivos específicos. São eles: identificar e reunir trabalhos que discutem sobre a utilização dos mais diversos tipos de Inteligência Artificial e sua utilização na Segurança Pública; identificar quais as principais técnicas e tecnologias de Inteligência Artificial utilizadas na Segurança Pública; explorar o uso de Inteligência Artificial na Segurança Pública; investigar quais os principais desafios e problemáticas da utilização de Inteligência Artificial na Segurança Pública; apresentar os resultados por meio da Revisão Sistemática da Literatura.

Uma revisão bibliográfica atualizada pode fornecer uma visão abrangente do estado da arte na utilização de IA na segurança pública, abordando as tendências mais recentes e os desafios emergentes. Compreender o cenário atual é fundamental para a compreensão dos avanços e limitações das tecnologias de IA aplicadas à segurança pública, bem como para a identificação de oportunidades de pesquisa e de aplicação prática.

1.1 Organização do trabalho

O trabalho está estruturado da seguinte maneira: no Capítulo 2 será apresentado o referencial teórico e o corpo principal da revisão sistemática da literatura. Essa parte do trabalho é responsável por apresentar os principais conceitos para fins de contextualização.

No Capítulo 3 é apresentada a metodologia. Nesta parte são apresentados os passos utilizados para alcançar os objetivos específicos previamente definidos.

No Capítulo 4 está descrito todo o planejamento utilizado na elaboração do presente trabalho. Neste capítulo encontram-se as *strings* de buscas utilizadas para obtenção dos materiais de estudo, os critérios de inclusão, exclusão e qualidade para seleção dos trabalhos obtidos, entre outros.

No Capítulo 5 estão exibidos os resultados e discussões. Nesse tópico, são apresentados os resultados das nossas buscas nas bases de dados, bem como discussões sobre eles.

No Capítulo 6 é apresentada a conclusão que incorpora nossos resultados apresentados de maneira concisa para melhor recapitulação do texto.

2. REFERENCIAL TEÓRICO

Neste capítulo, são apresentados os conceitos referenciais teóricos que tratam dos principais conceitos que dão suporte ao trabalho aqui realizado

2.1.1 Inteligência artificial

Há muitos debates acerca do conceito de IA. Muito dessa dificuldade deve-se ao fato de ser difícil definir exatamente o que é inteligência. Sobre IA, alguns definem como “máquinas que se comportam de forma semelhante a humanos ou são capazes de ações que necessitam de inteligência” (SAMOILI, 2020).

Para esse artigo, a definição que será utilizada de base é a feita pelo *High-level expert group*(HLEG).

“Sistemas de inteligência artificial são sistemas de software (e possivelmente também hardware) projetados por humanos que, ao receberem um objetivo complexo, atuam na dimensão física ou digital ao perceberem o ambiente por meio da aquisição de dados, interpretando os dados coletados estruturados ou não estruturados, raciocinando sobre o conhecimento, ou processando a informação derivada desses dados e decidindo a melhor ação a tomar para alcançar o objetivo dado. Os sistemas de IA podem usar regras simbólicas ou aprender um modelo numérico, e também podem adaptar seu comportamento ao analisar como o ambiente é afetado por suas ações anteriores.” (EUROPEAN COMISSION, 2021)

O aprendizado de uma IA tem como objetivo “ensinar máquinas a lidar com os dados de maneira mais eficiente.” (MAHESH, 2018). O autor, no mesmo artigo, complementa que “indústrias aplicam aprendizado de máquina para extrair dados relevantes. O propósito do aprendizado de máquina é aprender a partir dos dados.” e também que “A aprendizagem de máquina depende de diferentes algoritmos para resolver problemas de dados. [...] não há um único tipo de algoritmo que sirva para todos os casos, é o melhor para resolver um problema.”

Conforme dito por Schaal (2020), o processo de aprendizado de uma inteligência artificial de uma máquina pode ser dividido em algumas formas: “Aprendizado supervisionado, aprendizado não supervisionado, e semi supervisionado como os três estilos de aprendizado.”

Utilizando os conceitos de (MAHESH, 2018), pode-se conceituar essas três aplicações como:

- **Aprendizado supervisionado:** O aprendizado supervisionado é a tarefa de aprendizado de máquina de aprender uma função que mapeia uma entrada para uma saída com base em pares de entrada e saída de exemplo. Ele deduz uma função a partir de dados de treinamento rotulados, que consistem em um conjunto de exemplos de treinamento. Os algoritmos de aprendizado de máquina supervisionado são aqueles que necessitam de assistência externa.
- **Aprendizado não supervisionado:** é chamado de aprendizado não supervisionado porque, ao contrário do aprendizado supervisionado mencionado anteriormente, não há respostas corretas e não há um professor. Os algoritmos são deixados por conta própria para descobrir e apresentar uma estrutura interessante nos dados. Os algoritmos de aprendizado não supervisionado aprendem algumas características dos dados. Quando novos dados são introduzidos, eles usam as características previamente aprendidas para reconhecer a classe dos dados.
- **Aprendizado semi supervisionado:** O aprendizado de máquina semi-supervisionado é uma combinação de métodos de aprendizado supervisionado e não supervisionado. Pode ser frutífero em áreas de aprendizado de máquina e mineração de dados em que os dados não rotulados já estão presentes e obter dados rotulados é um processo tedioso. Com métodos mais comuns de aprendizado de máquina supervisionado, você treina um algoritmo de aprendizado de máquina em um conjunto de dados "rotulado", no qual cada registro inclui informações sobre o resultado.

Importante ressaltar que essas não são as únicas formas de aprendizado dentro do conceito de machine learning, mas sim as que mais englobam as outras menos populares.

2.1.2 ChatBOTS

Com a popularização das IAs, outras vertentes e aplicações do assunto surgiram com o tempo, entre elas os *Chatbots*. Define-se um *chatbot* como “um programa de computador designado para ter uma conversa com um ser humano,

principalmente pela internet.” (CHATBOT, 2023). Entende-se que os *chatbots* não são o único conceito que relaciona IA à segurança pública, porém são acessíveis o suficiente para a população média ter acesso.

Chatbots utilizam processamento de linguagem natural(PLN). O PLN é um conceito básico, análogo à IAs, e já existe há certo tempo, “[...] já na década de 50, pesquisas relevantes estavam sendo conduzidas e teorias foram criadas a respeito de como uma máquina pode se tornar capaz de interpretar a fala humana.” (KRUTILLA; KOVARI, 2022). Alguns exemplos de IAs que utilizam PLN, são assistentes virtuais mais antigas, como Siri, da Apple ou a Cortana, da Microsoft.

No caso dos *chatbots*, que são mais modernos, também são utilizados outros ramos da IA, como a Compreensão da linguagem natural (CLN), “a qual é utilizada desde os anos 60, como no projeto LUNAR, e é um sistema capaz de responder perguntas e realizar ações por meio de blocos de brinquedo em um ambiente, conforme citado por” (PERCY, 2016) e a geração de linguagem natural (GLN), que também possui várias aplicações por si só como: “resumo de dados, conseguir documentos preliminares, gerar explicações, gerar textos com fins de persuasão, entre outros” (MCDONALD, 2010) para que tenham sua característica de simular uma conversa real.

“Além de servirem para entreter as pessoas, os *chatbots* também tem utilidades em outros campos como educação, negócios, saúde e lazer” (SHAWAR & ATWELL, 2007). Os *chatbots* (e consequentemente o assunto de inteligência artificial) começaram a receber certa notoriedade com a popularização do CHAT GPT, uma IA poderosa capaz não só de manter conversas com grande fidelidade de um ser humano, mas também resolver diversos problemas, que podem ser expressados via texto, como por exemplo

- Questões de saúde pública(vacinação, detecção antecipada, construção de estilo de vida, etc.) (BISWAS, 2023);
- Ações de aprendizado educacionais (FIRAT, 2023);
- Resolução de problemas como bugs na área da programação (SURAMEERY, 2023);
- Segurança da informação (EDU,2022).

2.1.3 Segurança pública

Tradicionalmente, a segurança como um termo geral na política tem um papel dominante. A formalização da proteção dos bens, os quais incluem a vida, vêm desde os tempos mais antigos. De acordo com Bislev (2004) "escritos antigos mostram que as escritas tradicionais sobre soberania e segurança têm se concentrado na proteção física do estado soberano. No entanto, no modelo westfaliano, a segurança externa e interna na verdade andam de mãos dadas". Isso implica que a segurança do próprio estado como soberano e único "digno" de ser protegido é um conceito antiquado. A proteção da ordem social tem a mesma relevância no processo, conceito chave para a compreensão da segurança pública em geral

De acordo com a compreensão de Weber no livro "Economia e Sociedade", o Estado é a única instituição que tem o direito de utilizar da violência. Ao interpretar essa afirmação de maneira literal, entende-se como a segurança pública é importante para o meio social. A proteção do estado para com os seus é tão relevante, que suas ações justificam os meios.

Conforme dito por Costa (2010, p.131) conceitua-se a segurança pública como:

"Conjunto integrado e otimizado envolvendo instrumentos de coação, justiça, defesa dos direitos, saúde e social. O processo de segurança pública se inicia pela prevenção e finda na reparação do dano, no tratamento das causas e na reinclusão na sociedade do autor do ilícito."

Entende-se que ao ser aplicada em uma "sociedade democrática plena, a SP não vai de contraponto à liberdade, mas sim um dos caminhos que trafega para a qualidade de vida dos cidadãos" (VEDOVA, 2018).

2.1.4 Segurança pública x Inteligência artificial

O uso de inteligência artificial no governo vem ascendendo com as suas diferentes aplicações: automatização de ações, decisões entregues por *chatbots*, entre outros. De acordo com Xavier (2020), diversas cidades no Brasil enfrentam problemas crônicos de segurança pública e a utilização de inteligência tem como objetivo auxiliar as decisões dos governantes e agentes de segurança a obter melhores resultados no atendimento de ocorrências e prevenção criminal. Conforme

discutido por Graham and Wood (2003), a utilização de tecnologias digitais para a vigilância de ambientes, possibilitou transformar e traduzir o espaço físico em um ambiente controlável. O uso de IAs, segundo Henman (2020) possui três aplicações fundamentais na segurança pública: detectar padrões, organizar populações e realizar previsões. No primeiro caso, os algoritmos mais modernos conseguem operar de maneira precisa, diferente de seres humanos que não possuem essa capacidade com tanta velocidade. Cita-se por exemplo esse uso na combinação de padrões de DNA, para detectar doenças. No segundo caso, IAs podem dividir populações das mais diferentes categorias. Uma tarefa que, novamente, é feita com muito mais rapidez nesse caso. Por último, o modelo de previsão é capaz de encontrar possíveis finais, baseados no treinamento que a IA recebeu. Pode-se exemplificar com casos policiais, que com os padrões recebidos de tipos, locais e frequência de crimes consegue detectar possíveis ações em potencial.

Conforme os portais informativos Forbes e *Intelligence automation network*. Existem algumas aplicações de inteligência artificial que, entre as possíveis, podem ser inseridas na segurança pública. Cita-se:

- **Reconhecimento facial:** Conforme dito por Smith (2020), Reconhecimento da Biometria Facial é uma das tecnologias de IA mais significantes para propósitos de segurança. Tal tecnologia possibilita a utilização em diversos segmentos da SP. Pode ser utilizada mediante a necessidade da identificação de autores, vítimas ou testemunhas relacionadas a algum fato criminoso, além de poder auxiliar na busca de pessoas desaparecidas. Outro uso é para o monitoramento e controle de acesso, como, por exemplo, a linha BIO-T da Intelbras, lançada em 2022.
- **Inclusão de *blocklists*:** juntamente com a ideia de reconhecimento facial, podem ser criados padrões com a ajuda de *machine learning* para colocar indivíduos em listas de bloqueio. Dessa maneira o trabalho policial para identificar e deter criminosos é facilitado.
- **Deteção de acessórios na cabeça (como capacetes ou balaclavas):** Conforme citado pelo autor Gryfo (2020), em seu artigo para o *Médium*, é uma aplicação bastante útil para estabelecimentos comerciais e residências, por exemplo, tendo em vista que a utilização desses acessórios é uma prática regular em roubos e furtos.

- **Reconhecimento militar geral:** Ao utilizar conceitos como reconhecimento facial ou *blacklists*, forças militares podem facilmente localizar e eliminar possíveis ameaças, como em casos de conflitos ou invasões terroristas.
- **Detecção de bombas por meio de padrões:** Uma startup israelense nomeada UVEye desenvolveu um sistema capaz de detectar anomalias como itens traficados ou bombas por meio de *machine learning* e inteligência artificial.

“O sistema utiliza câmeras de alta resolução estrategicamente posicionadas para criar uma imagem 3D de anomalias, como dispositivos explosivos improvisados, armas ilegais, drogas e outros materiais suspeitos. A UVEye afirma que a tecnologia funcionará mesmo quando o veículo estiver se deslocando a até 28 MPH, o que significa que a tecnologia pode detectar objetos que de outra forma passariam despercebidos pelo olho humano.” (MUSPRATT, 2018)

- **Controle de tráfego:** A utilização de IA para monitoramento de tráfego traz consigo benefícios cruciais para melhor funcionamento da cidade. O Centro de Gerenciamento e Operação de Tráfego Urbano do Departamento de Transporte da Cidade de Ho Chi Minh, já tem aplicado inteligência artificial para gerenciamento de tráfego. “[...] tem sido implementada e alcançado muitos resultados importantes, contribuindo para o desenvolvimento da cidade, reduzindo a congestão do tráfego e diminuindo acidentes de trânsito” (CONG, 2023).

2.1.5 Racionalidade

A racionalidade humana possui inúmeras complexidades, contudo, a racionalidade de IAs pode ser facilmente identificada, uma vez que estas operam a partir de procedimentos lógicos e matemáticos.

” [...] se tornaram superportadores de racionalidade formal, de duas maneiras. Primeiramente, eles podem melhorar a si mesmos ao desempenhar suas tarefas; nesse sentido, os algoritmos podem “aprender”. Dadas restrições e/ou condições de fronteira, eles trabalham para encontrar a solução logicamente ou matematicamente “correta” em um conjunto de dados e, ao receberem mais dados, são capazes de desenvolver uma solução “mais correta”. Além disso, os algoritmos são superportadores devido à velocidade sem precedentes, mesmo em tempo real, de

processamento de grandes volumes de "*big data*" para produzir ou calcular resultados[...]" (LINDEBAUM et al., 2020)

2.1.6 Ética

É certo que essas tecnologias podem ser usadas para o bem, mas de maneira semelhante podem ser usadas para o mal. Conforme citado por Brundage (2018), IAs podem possuir certas capacidades que facilitam esse processo. Elas podem: Exceder capacidades humanas, aumentar o anonimato, se desenvolver rapidamente com difusão rápida, facilidade de se explorar sua natureza como bem desejar, disseminação de notícias falsas, campanhas de influência automáticas, entre outros.

A questão da ética se torna um problema ao compreender que uma IA só pode ser o que é ao aprender. Inicialmente, essas máquinas tinham que ser devidamente instruídas, mas atualmente conceitos como "métodos de aprendizado profundo (*deep learning*) geralmente extraem e aprendem características de forma orientada por dados, com pouca ou nenhuma participação humana." (YANG, 2019)

As IAs vêm evoluindo numa velocidade exponencial considerável, o que aumenta ainda mais a discussão. Atualmente, elas possuem um grande potencial de realizar as mesmas atividades que humanos:

"A automação deu um salto à frente com a recente introdução de ferramentas de IA generativa. "Generativa" refere-se ao fato de que essas ferramentas conseguem identificar padrões em conjuntos enormes de dados e gerar novo conteúdo — uma habilidade que frequentemente foi considerada exclusivamente humana." (ELLINGRUD, 2023)

2.1.7 Inteligência artificial e ética

As questões éticas que concernem às IAs estão relacionadas com o ciclo de vida completo de tais sistemas, desde a pesquisa, design e desenvolvimento, até implementação, uso, manutenção, comércio e término (UNESCO, 2022).

Apesar dos inúmeros benefícios relacionados à utilização da IA, surgem problemáticas em relação a esse uso:

- Conforme citado por Garcia (2020), os sistemas de IA podem herdar preconceitos presentes nos dados de treinamento, levando a decisões

discriminatórias;

- A coleta massiva de dados para treinamento de algoritmos de IA levanta preocupações sobre a privacidade e a segurança das informações pessoais, principalmente nos casos em que não há consentimento, como exposto por Solon e Levin (2018);
- Discutido por Pennycook e Rand (2019), as IAs podem ser utilizadas para disseminação de *fake news*, desta maneira, influenciando a opinião pública;
- *Accountability*: a falta de mecanismos transparentes para a identificação do indivíduo ou entidade responsável por eventuais danos decorrentes de uma solução de IA (BIRD et al., 2020; MULLER, 2020).

2.1.8 Cidades inteligentes(*smart cities*)

Quando se trata da aplicação de IAs ou outras tecnologias quaisquer é difícil não citar as cidades inteligentes. O conceito de cidades num geral ainda flutua bastante, mas de uma visão semântica Lacoste (2005) exemplifica com clareza.

“A palavra cidade vem do latim "civitate", noção próxima de "civitas" que deu origem às palavras cidadão e civilização. A palavra urbano vem do latim "urbs", que também significa cidade. Já a palavra grega "polis", cidade e "politikos", da cidade, deram origem a palavra política. Finalmente a noção de aglomerado vem do latim "glomus, glomero" e significa bola ou fazer em bola” (LACOSTE, 2005, p. 21, 80, 315).

Quanto à definição de cidades inteligentes, alguns estudiosos no assunto afirmam que “O termo serve para definir cidades que enfatizaram seu processo de urbanização em tecnologia, pesquisa, globalização e inovação” (YIN, 2015).

O uso de IAs em cidades possui aplicações quase ilimitadas. Muitas formas de se utilizar surgem a cada dia e a necessidade de crescimento fomenta ainda mais essa aplicação. “A tecnologia de inteligência artificial e as cidades, garantindo a integração de dimensões fundamentais de Cultura, Metabolismo e Governança” (ALLAM, 2019)

3. METODOLOGIA

Este trabalho faz parte de uma Revisão Bibliográfica(RB). A RB, segundo Gil (2002), é constituída pela análise e interpretação de dados, sobretudo, dos advindos de material impresso, como livros, periódicos, imagens, manuscritos, entre outros. Para ele, “Os livros constituem as fontes bibliográficas por excelência” e podem ser classificados como de leitura corrente ou de referência. “Os livros de leitura corrente abrangem as obras referentes aos diversos gêneros literários (romance, poesia, teatro etc.) e também as obras de divulgação, isto é, as que objetivam proporcionar conhecimentos científicos ou técnicos.”. Acerca dos livros de referência, “ também denominados livros de consulta, são aqueles que têm por objetivo possibilitar a rápida obtenção das informações requeridas, ou,então, a localização das obras que as contêm.” (GIL, 2002, p. 44).

Ainda de acordo com Gil (2002):

[...] a principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura de uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente. Essa vantagem torna-se particularmente importante quando o problema de pesquisa requer dados muito dispersos pelo espaço. Por exemplo, seria impossível a um pesquisador percorrer todo o território brasileiro em busca de dados sobre população ou renda per capita; todavia, se tem a sua disposição uma bibliografia adequada, não tem maiores obstáculos para contar com as informações requeridas. A pesquisa bibliográfica também é indispensável nos estudos históricos. Em muitas situações, não há outra maneira de conhecer os fatos passados se não com base em dados bibliográficos.

Na sequência, são apresentados, detalhadamente, os passos que foram utilizados para a realização deste trabalho:

Passo 1: Revisão de Literatura Multivocal

A Revisão de Literatura Multivocal(RLM) é um tipo de revisão de literatura composta por todo tipo de escrita disponível sobre algum assunto. (OGAWA; MALEN, 1991). Por ser todo tipo de escrita, inclui também a chamada Literatura Cinzenta(LC) (em inglês, *Grey Literature*). LC pode ser definida como “aquela que é produzida em todos os níveis governamentais, acadêmicos, de negócios e

industriais em meios eletrônicos e impressos não controlados por editoras comerciais”(AUGER, 1998).

Como fonte de Literatura Cinzenta, foi realizada uma busca em portais de notícias, blogs informativos, jornais, entre outros.

Os resultados da revisão e das buscas na Literatura Cinzenta são apresentados no tópico 4.1.

Passo 2: Identificação das principais técnicas, tecnologias e problemáticas advindas da utilização de IA na SP

A partir da leitura dos trabalhos selecionados seguindo os critérios de inclusão, exclusão e qualidade, apresentados na seção 4.1.5 aplicados nas buscas utilizando as *strings* do Quadro 1, foi realizado um levantamento das principais técnicas e tecnologias de IA que eram utilizadas nos âmbitos de monitoramento, prevenção e SP geral. Os trabalhos foram buscados nas bases de dados descritas no tópico 4.1.4, bem como na literatura cinzenta.

Os resultados desse levantamento são apresentados a partir do tópico cinco.

Passo 3: Resultados e Discussão - Questão primária

A partir dos resultados obtidos no Passo 2, os principais temas e utilizações foram utilizados na construção das *strings* descritas no Quadro 2. Os resultados desta segunda busca foram então utilizados para responder as QPs.

A QP1 foi respondida utilizando os resultados obtidos e separando-os entre os trabalhos em Língua Portuguesa e os de Língua Inglesa. Num primeiro momento, os dados foram apresentados de forma quantitativa, e para maior clareza e facilidade de visualização, foi elaborado um gráfico a partir da quantidade de trabalhos retornada.

Posteriormente, os principais temas foram então destrinchados, buscando explicar e evidenciar as principais características, técnicas e métodos de cada um.

Passo 4: Resultados e Discussão - Questão secundária

Para desenvolvimento da discussão sobre ética e problemáticas, respondendo a QP2, foi utilizada a conceituação de racionalidade contida no referencial teórico. Quando relacionada à IAs, a ética se apresenta com alguns

problemas que vêm sendo discutidos e levantados nesses últimos anos devido à popularização dessa nova forma de inteligência. Dito isto, a presente RSL buscou elucidar as principais questões éticas e pontuar as problemáticas que circundam esta utilização de IA na SP.

Os dados finais foram coletados de maneira passiva, com trabalhos que contribuem tanto para os temas principais, quanto para a ética da utilização dessas tecnologias na segurança pública. As ideias mais relevantes foram sintetizadas no tópico 5.1.2

4. PLANEJAMENTO DA REVISÃO

4.1 Revisão de literatura multivocal

A Revisão de Literatura Multivocal(RLM) é um tipo de revisão de literatura composta por todo o tipo de escrita disponível sobre algum assunto. (OGAWA; MALEN, 1991). Por ser todo tipo de escrita, inclui também a chamada Literatura Cinzenta(LC) (em inglês, *Grey Literature*). LC pode ser definida como “aquela que é produzida em todos os níveis governamentais, acadêmicos, de negócios e industriais em meios eletrônicos e impressos não controlados por editoras comerciais” (AUGER, 1998).

4.1.1 Revisão Narrativa de literatura

“Os artigos de revisão narrativa são publicações amplas, apropriadas para descrever e discutir o desenvolvimento ou o "estado da arte" de um determinado assunto, sob ponto de vista teórico ou contextual.” (ACTA PAULISTA DE ENFERMAGEM, 2007).

A presente RSL segue o seguinte planejamento: a) definição do tipo de revisão b) objetivos e questões de pesquisa, c) definição das *strings* de busca, d) definição dos motores de busca utilizados, e) definição dos critérios de inclusão, exclusão e qualidade, f) definição dos métodos de seleção de trabalho, h) análise dos trabalhos e, por fim, i) trabalhos da LC.

4.1.2 Objetivos e questões de pesquisa

O objetivo desta revisão é expor as vantagens e desvantagens, utilizações e possibilidades, implicações éticas e sociais do uso de IAs no setor da SP. As questões

- **Questão Primária (QP):** A questão primária da presente revisão é: Quais são as principais aplicações de IA na SP?
- **Questão Secundária (QS):** A questão secundária a ser discutida na presente revisão é: Quais as principais problemáticas das aplicações e ferramentas de IA na SP?

4.1.3 Strings de busca

As *strings* de busca são termos e palavras-chaves que serão utilizados para encontrar trabalhos que tratam do tema desejado. Tais *strings* podem ser compostas por aspectos lógicos, utilizando os operadores *booleanos AND* e *OR*, para melhor especificidade e precisão das buscas nas bases de dados. “Para criar a *String* de busca é necessário identificar as palavras e termos referente ao tema de pesquisa. Isso pode ser feito a partir do estudo preliminar das fontes (artigos) e também por consulta a especialistas e pesquisadores.” (AMARAL, 2011).

As buscas por trabalhos foram realizadas tanto em Língua Portuguesa quanto na Língua Inglesa, e basearam-se principalmente nos seguintes termos: “Inteligência artificial”, “segurança”, “segurança pública”, “ética”, “*artificial intelligence*”, “*security*”, “*public surveillance*”, “*ethics*”, “*chatbots*”, “*public security*”.

Com base nesses termos, foram criadas as seguintes *strings*:

Quadro 1: Strings de busca

Google Acadêmico	("Systematic Review" OR "Revisão Sistemática") AND ("Artificial Intelligence" OR "Inteligência Artificial") AND ("Public Security" OR "Public Surveillance" OR "Segurança Pública") ("Inteligência artificial" OR "Artificial intelligence") AND ("Segurança pública" OR "Segurança" OR "Public security" OR "Public surveillance"); ("Inteligência artificial" AND ("Segurança pública" OR "Segurança")) OR ("Artificial Intelligence AND ("Public security" OR "Public surveillance")) Artificial intelligence AND Public Security AND Systematic Review "Chatbots" AND ("Public Security" OR "Public Surveillance") AND "Systematic Review"
	("Inteligência artificial" OR "Artificial intelligence") AND ("Ética" OR "Ethics")
	("Inteligência artificial" OR "Artificial intelligence") AND ("Segurança pública" OR "Segurança" OR "Public security" OR "Public surveillance") AND ("Ética" OR "Ethics")

	"Chatbots" AND ("Segurança pública" OR "Segurança" OR "Public security" OR "Public surveillance")
--	---

Fonte: Autores (2023)

As *strings* contidas no Quadro 1 foram utilizadas para a busca inicial dos trabalhos, que visava introduzir o tema e também encontrar os principais conceitos e aplicações de IA na SP. Ademais, também foram realizadas buscas em fontes de LC. Nestas, foram utilizados termos como "inteligência artificial para monitoramento", "*chatbots* na segurança pública" e "inteligência artificial na segurança pública".

Quadro 2: Strings utilizadas para obtenção da quantidade total de trabalhos

Termo	String
Smart Policing	("Artificial Intelligence" OR "Inteligência Artificial") AND ("Smart Policy" OR "Smart Policing" OR "Predictive Policing" OR "Policiamento preditivo" OR "Policiamento Inteligente") AND ("Public Security" OR "Public Surveillance" OR "Segurança Pública")
CCTV	("Artificial Intelligence" OR "Inteligência Artificial") AND ("Circuito fechado de televisão" OR "Closed-circuit television" OR "CCTV" OR "CFTV") AND ("Public Security" OR "Public Surveillance" OR "Segurança Pública")
Smart Cities	("Artificial Intelligence" OR "Inteligência Artificial") AND ("Smart City" OR "Smart Cities" OR "Cidade Inteligente" OR "Cidades Inteligentes") AND ("Public Security" OR "Public Surveillance" OR "Segurança Pública")
Cyberattack	("Artificial Intelligence" OR "Inteligência Artificial") AND ("Cyberattack" OR "Ciberataque") AND ("Public Security" OR "Public Surveillance" OR "Segurança Pública")
Drone/UAV	("Artificial Intelligence" OR "Inteligência Artificial") AND ("Drone" OR "VANT" OR "UAV") AND ("Public Security" OR "Public Surveillance" OR "Segurança Pública")
Chatbot	("Artificial Intelligence" OR "Inteligência Artificial") AND ("Chatbot") AND ("Public Security" OR "Public Surveillance" OR "Segurança Pública")

Fonte: Autores (2023)

As strings do Quadro 2, por sua vez, foram utilizadas para obter os dados totais do estado da arte atual das pesquisas sobre IA em relação a SP. Nota-se que

as strings também continham os termos em português, buscando, assim, maior abrangência e totalidade dos dados.

4.1.4 Motores de busca

De acordo com Quintana (2012), os motores de busca são ferramentas indispensáveis na pesquisa de informação na web. A sua finalidade é fornecer resultados relevantes aos seus utilizadores de modo que fiquem satisfeitos. Uma das formas de o conseguirem é através da indexação, que lhes permite guardar informação útil. Dito isso, o motor de busca utilizado para esse trabalho foi o Google acadêmico para os trabalhos de relevância acadêmica e portais de notícias, vídeos disponíveis em plataformas como o Youtube, manuais, blogs informativos e jornais para os trabalhos relacionados à literatura cinzenta.

4.1.5 Critérios de inclusão, exclusão e qualidade

Quadro 3: Critérios de inclusão e exclusão de trabalhos

Critérios de inclusão		Critérios de exclusão		Critérios de qualidade	
CI1	Trabalhos escritos em inglês ou português	CE1	Trabalhos publicados antes de 2018	CQ1	Material consistente
CI2	Material coerente com o tema	CE2	Trabalhos incompletos	CQ2	Materiais com transparência no assunto
CI3	Material coerente com os tipos de fontes propostos	CE3	Trabalhos duplicados	CQ3	Material com fontes diversificadas
		CE4	Trabalhos em qualquer outra linguagem que não seja português ou inglês	CQ4	Relevância do tema tratado
		CE5	Trabalhos com grau de obsolescência elevada		
		CE6	Trabalhos com viés excessivo		

Fonte: Autores (2023)

Os trabalhos que foram aceitos devem ao menos atender aos critérios de

inclusão e não devem atender nenhum dos critérios de exclusão. Os critérios de qualidade definem parâmetros opcionais, que agregam na hora da seleção mas não definem sua escolha. É de suma importância ressaltar que os critérios de avaliação foram utilizados apenas na busca preliminar de trabalhos.

4.1.6 Métodos de seleção de trabalho

A seleção dos trabalhos advindos das buscas foi feita mediante as etapas seguintes:

- **1ª Etapa:** Nesta etapa da seleção, todas as *strings* de busca descritas no tópico 4.1.4 foram aplicadas na busca no Google Acadêmico. Também foram aplicados os critérios CI1 e CI2 para complementar a filtragem dos trabalhos.
- **2ª Etapa:** Os artigos selecionados na primeira etapa são então submetidos a análise do título, resumo e também conclusão, para validação da relevância do tema abordado para esta RSL, conforme descrito no CQ4.
- **3ª Etapa:** Por fim, os trabalhos aprovados nas etapas prévias, serão analisados novamente e, desta vez, mais criteriosamente. Os trabalhos tiveram a qualidade da escrita, coesão e coerência, entre outros. Outrossim, também foram reaplicados todos os CIs, CEs e CQs. Os trabalhos aprovados nessa etapa foram utilizados na composição do presente trabalho.

4.1.7 Análise dos trabalhos

O trabalho escrito por Zuiderwijk (2021) possui como tema a aplicação do uso de inteligência artificial na governança pública. Os objetivos do trabalho consultado são três: 1)Posicionar a pesquisa identificada em relação ao conhecimento existente, 2)Obter *insights* úteis sobre os métodos de pesquisa que outros acadêmicos têm utilizado para estudar as implicações do uso de IA no governo para a governança pública. e 3)Obter *insights* úteis sobre as implicações do uso de IA no governo para a governança pública.

O autor, ao apresentar resultados, os dividiu em diferentes tabelas. A Figura 3 é responsável por anexar a referência do trabalho selecionado juntamente com o seu objetivo de maneira resumida

Figura 3 - Recorte da visão geral dos estudos incluídos em nossa revisão sistemática da literatura

Table 3

Overview of studies included in our systematic literature review.

#	Reference	Study objective
1	Al-Mushayt (2019)	To propose a framework that utilizes AI (more specifically an AI-enabled chatbot) to improve citizen-government communication and services
2	Alexopoulos et al. (2019)	To identify benefits and obstacles towards the adoption of the ML [Machine Learning] innovative technology and the identification of ML approaches in the public sector
3	Androutsopoulou, Karacapilidis, Loukis, and Charalabidis (2019)	To present a novel approach along with the architecture of a supporting ICT platform for the use of AI technology (chatbots) in the public sector for improving communication between government and citizens
4	Aoki (2020)	To investigate the public's initial trust in so-called "artificial intelligence" (AI) chatbots about to be introduced into use in the public sector

Fonte: (ZUIDERWIJK, 2021)

Já na Figura 4, como forma de expor de maneira complementar o autor separa os trabalhos com temas ligados à proposta do seu artigo.

Figura 4: Recorte de benefícios em potencial do uso de IA no governo, identificados nos estudos exemplificados.

Table 4

Potential benefits of AI use in government, as identified in the studies in our sample.

Category	Potential benefits
1) Efficiency and performance benefits	Efficiency (Bullock, 2019; Gomes de Sousa et al., 2019; Toll et al., 2019; Valle-Cruz et al., 2019) Efficiency resulting from Machine Learning in particular (Alexopoulos et al., 2019) Effectiveness (Bullock, 2019) More efficient e-government services and systems (Al-Mushayt, 2019) More efficient government operations (Ojo et al., 2019) Efficient process and task automation (Ojo et al., 2019) Greater programme efficacy (Ojo et al., 2019) Error reduction (Valle-Cruz et al., 2019) Performance and process simplification resulting from Machine Learning in particular (Alexopoulos et al., 2019) Automation (Valle-Cruz et al., 2019) Automating processes (Toll et al., 2019) Reduce administrative burdens (Wirtz et al., 2019) Scalability (for Machine learning in particular) (Alexopoulos et al., 2019) AI could relieve resource constrained organizations from mundane and repetitive tasks (Kuziemski & Misuraca, 2020)

Fonte: (ZUIDERWIJK, 2021)

O segundo artigo (SHIDIK, 2019), como uma revisão de literatura, discorre sobre o assunto de maneira mais específica. A temática se resume exclusivamente a vigilância utilizando vídeo inteligente neste artigo. O autor destaca que diversas áreas já fazem uso desses serviços de vigilância, como: prevenção de crimes, monitoramento de aeroportos, cuidados com idosos e monitoramento e controle de importantes avenidas e infraestruturas. Nesta temática, foram identificados cinco tipos de utilização da vigilância inteligente:

- **Proteção e privacidade:** relacionado a implementação nas mais diversas áreas, cuidados com idosos, monitoramento de segurança em museus, trens, bancos, aeroportos, etc.
- **Deteccção de objetos e rastreamento:** engloba monitoramento e

rastreamento de pedestres, identificação de pessoas e monitoramento de ambientes caóticos;

- **Reconhecimento e compreensão comportamental:** classificação de veículos móveis, contar objetos, entre outros;
- **Controle e monitoramento de tráfego:** diz respeito a estimativa do tráfego de veículos, prevenção de acidentes de trânsito e classificação dos veículos;
- **Monitoramento de acidentes e desastres:** diz respeito a atividades preventivas, como identificação de incêndios, detecção de enchentes, entre outros.

Quanto ao impacto que as IAs estão tendo e que podem vir a ter no âmbito de serviços públicos, o trabalho de Henman(2020) aborda algumas questões. Dentre as ramificações discutidas, estão: tomada de decisões automática, *chatbots*, governança e segurança públicas, entre outros. Quanto à tomada de decisões, o autor destaca três formas de operação: detecção de padrões, classificação populacional; e fazer previsões. No que diz respeito a classificação populacional, é comentado que, por consequência da criação e reconhecimento de padrões, IAs são capazes de separar indivíduos em diferentes grupos ou categorias, de acordo com diferentes resultados, pontuações ou riscos. Para efeito de comprovação, é citado sobre o Secure Flight.

"*Secure Flight* é um programa de pré-seleção de passageiros com base em riscos que aprimora a segurança ao identificar passageiros de baixo e alto risco antes de chegarem ao aeroporto. O programa faz isso comparando os nomes dos passageiros com listas de viajantes confiáveis e listas de observação. Para proteger a privacidade, o programa *Secure Flight* coleta a quantidade mínima de informações pessoais necessárias para realizar a correspondência efetiva, que inclui nome completo, data de nascimento e gênero. Além disso, impede que indivíduos nas listas de Observação de Terroristas,[...] embarquem em qualquer aeronave."

Na publicação do autor Christopher Rigano (2019) é demonstrada uma interessante figura do plano estratégico para a tecnologia nos Estados Unidos da América(EUA). A publicação foi feita pela própria casa branca, em 2016 e mostra os planos e intenções da aplicação da inteligência artificial nas seguintes áreas: 1) Manufatura, 2) logística, 3)finança, 4)transporte, 5) agricultura, 6) marketing, 7) comunicação, 8) ciência, 9) tecnologia, 10) educação, 11) medicina, 12) lei, 13)

serviços pessoais, 14) aplicações de lei e segurança e 15) segurança e predição.

A utilidade das previsões e planos de números 12), 14) e 15) incluem ideias relevantes para o tema tratado no trabalho. São elas, respectivamente:

- Analisar o histórico de jurisprudência;
- Auxiliar no processo de descoberta;
- Resumir as evidências;
- Detectar padrões e comportamentos anômalos ;
- Prever o comportamento de multidões e padrões criminais ;
- Proteger infraestruturas críticas ;
- Desvendar redes criminosas;
- Prever interrupções na infraestrutura com sistemas de sensores distribuídos e informações de padrões;
- Adaptar operações para impacto mínimo.

Visualizando o potencial das IAs no policiamento e conseqüentemente na segurança pública como um todo, o autor declara:

“Ao usar a inteligência artificial e análises de policiamento preditivo integradas com respostas assistidas por computador e empresas de vídeo de segurança pública ao vivo, as forças policiais serão capazes de responder melhor a incidentes, prevenir ameaças, realizar intervenções, alocar recursos de maneira eficaz, investigar e analisar atividades criminosas. A inteligência artificial tem o potencial de se tornar uma parte permanente de nosso ecossistema de justiça criminal, fornecendo assistência nas investigações e permitindo que profissionais da justiça criminal mantenham melhor a segurança pública.” (RIGANO, 2019)

Os trabalhos citados acima abordam temas semelhantes ao proposto nesta monografia e também uma estrutura próxima à proposta. Ao buscar pelo tema da inteligência artificial e suas diferentes aplicações nota-se uma carência de revisões de literatura com esse tema em específico atualizadas e em português, sendo que outros temas possuem mais atenção para esse método como governança pública (exemplo acima), saúde, inovação, entre outros.

4.1.8 Busca na Literatura Cinzenta

Nesta seção são apresentadas publicações em blogs, jornais, entre outros

tipos de literatura cinzenta, que tratam sobre a utilização de *chatbots* e algumas técnicas de IA para auxiliar na segurança. Trabalhos encontrados são apresentados nos tópicos seguintes.

4.1.9 AI For Smart Policing

Segundo Chauhan (2023), o crime está em todo lugar. Todos os departamentos de polícia têm uma função principal: Manter o crime sob controle e consequentemente trazer a segurança pública. O autor levanta questões sobre o policiamento inteligente com a ajuda de IAs e levanta as principais questões que estão ao redor do tema: Vantagens, desvantagens, consequências, desafios e predições. Ao discorrer sobre esses assuntos, o autor também levanta questões relevantes para a proposta desse trabalho que respondem nossas questões primárias e secundárias que, respectivamente, dizem respeito à uma ferramenta específica para a segurança pública e também as questões éticas de se implementar IAs na SP

Verifica-se que a ênfase a um nicho específico do tema deste trabalho traz alguns exemplos que servem de complemento para a discussão como um todo, como progresso de utilização de IAs por diferentes forças policiais como Maharashtra, Jharkhand e Kolkata.

Por fim, vale ressaltar que a publicação do jornal digital “Legal service India” dá mais foco nos problemas vindos do país asiático, algo que não deixa o tema irrelevante, mas sim um pouco distante visto a discrepância cultural não só com o Brasil, mas com muitos países ocidentais.

4.1.10 Using Chatbot Technology to Improve how Law Enforcement Responds to Victims of Residential Burglary

O instituto de pesquisa RTI International identificou que as vítimas de furto domiciliar geralmente não recebiam a mesma atenção da lei como vítimas em comparação a outros crimes mais violentos. De acordo com *Bureau of Justice Statistics*, menos de 5% das vítimas desse tipo de crime recebiam assistência. Como forma de trazer melhoria para esses casos, desenvolveram o *chatbot Enhanced Virtual Victim Assistance (EVVA)*(em português, Assistente Virtual Melhorado para

Vítimas).

“[...]*chatbot* a que uma vítima pode recorrer para obter respostas a perguntas específicas e comuns relacionadas à sua experiência, e para obter encaminhamentos para órgãos nacionais e locais que podem fornecer recursos adicionais e assistência”

O principal benefício que pode ser identificado a partir da utilização de *chatbots* para denúncias de crimes, é o aumento na eficiência e rapidez do atendimento à vítima, respondendo à perguntas comumente realizadas e já providenciando a conexão com as autoridades locais, diminuindo, assim, o trabalho dos detetives e investigadores, bem como prover à vítima maior confiança no serviço da polícia.

4.1.11 Artificial intelligence bolsters public safety & security in smart cities

A autora Ruvalcaba (2023) faz um paralelo entre a SP e a comunicação veloz que as IAs permitem. Mesmo com o fluxo elevado de dados, a ajuda de IAs permite uma filtragem para melhor resultado. A ideia é que as IAs possuam uma aplicação mais passiva nas suas diversas atuações, servindo como um apoio

“A abundância de informações disponíveis hoje apresenta desafios importantes. À medida que as cidades implantam mais câmeras, sensores e outros dispositivos, elas aumentam a quantidade de informações que chegam. Isso pode se tornar avassalador para o pessoal de segurança, especialmente quando eles devem monitorar ativamente todas as entradas desses dispositivos para identificar ameaças específicas.” (RUVALCABA, 2023)

O artigo conclui com o importante lembrete que nesse fluxo de dados o elemento humano é crucial. Quem define realmente a validade, a instrução da máquina e a importância é - e deve - ser um elemento humano.

5. RESULTADOS DA RLM

O objetivo dessa RLS é apresentar as possíveis vantagens, desvantagens e aplicações do uso de inteligência artificial na segurança pública. Dessa maneira foram coletados um total de 22 trabalhos relevantes para as nossas questões de pesquisa. Foram utilizados 19 trabalhos que pudessem atender nossa QP, e 3 trabalhos que atendiam nossa QS, todos seguindo à risca os nossos CIs, CEs e CQs descritos no tópico no 4.1.5. Vale ressaltar que tratar sobre ética não era um requisito para seleção dos trabalhos.

Quadro 4: Listagem dos trabalhos encontrados, mostrando qual o tema e também as principais técnicas utilizadas (quando houver).

Referência		Tema	Técnicas citadas	Aplicações
1	ZEADALLY, S. et al. Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity . IEEE Access, v. 8, p. 1–1, 2020.	Exploração do potencial do uso de IAs melhorando soluções de cibersegurança, identificando fraquezas e forças	Machine learning, deep learning, árvores de decisões, K-ésimo Vizinho mais Próximo, redes neurais artificiais, Mapas de Kohonen	Aplicar as técnicas em: Internet, ataques de redes de BOTNET, vulnerabilidades em IOT
2	CONG, V. T. et al. APLICAÇÃO DE INTELIGÊNCIA ARTIFICIAL E DISPOSITIVOS DE MONITORAMENTO SOBRE PREVENÇÃO DE CRIMES DE DESORDEM PÚBLICA E CONDUTA DESORDEIRA . Lex Humana (ISSN 2175-0947), v. 15, n. 1, p. 59–70, 30 jan. 2023.	Apresenta algumas questões urgentes e fundamentais para a aplicação de inteligência artificial e dispositivos de monitoramento público na prevenção de distúrbios públicos, crimes e condutas desordenadas no presente e no futuro próximo.	Não especificado	Aplicação em CCTV, monitoramento e análise de dados
3	SPANAKI, K. et al. Artificial intelligence and food security: swarm intelligence of AgriTech drones for smart AgriFood operations. Production Planning &	O estudo propõe aplicações de inteligência artificial na segurança de alimentos/fazendas	Não especificado	Utilização de drones inspirados em bandos de pássaros para vigilância em locais de difícil acesso

	Control , p. 1–19, 25 fev. 2021.			
4	Chatbots for Law Enforcement – Enhanced Virtual Victim Assistant RTI. Disponível em: < https://www.rti.org/impact/chatbots-for-law-enforcement >. Acesso em: 28 nov. 2023.	Utilização da tecnologia <i>Chatbot</i> para melhorar a forma como as autoridades policiais respondem às vítimas de roubo residencial	<i>Chatbot</i> , Machine Learning	Facilitar e agilizar o processo de denúncia e suporte às vítimas de roubo residencial.
5	THAKUR, N. et al. Artificial Intelligence Techniques in Smart Cities Surveillance Using UAVs: A Survey . p. 329–353].	Tecnologias de Inteligência Artificial em <i>Smart Cities</i> para vigilância utilizando VANTs	CCTV, IoT, UAV, Deep Learning	Utilização de VANTs para vigilância em <i>smart cities</i> .
6	SOUSA, W. G. DE et al. How and where is artificial intelligence in the public sector going? A literature review and research agenda . Government Information Quarterly, v. 36, n. 4, p. 101392, jul. 2019	Utilização de IA no setor público como um todo, incluindo segurança	Modelagem preditiva	Avaliação de risco de fraude, identificação de áreas possivelmente mais perigosas e auditorias automatizadas
7	DE FERRAN, Cristianna M.; MOTTA, Claudia LR. Uso de Computação Cognitiva no Processo Semântico de um Atendente Virtual: Uma Aplicação na área da Segurança Pública . In: Anais Estendidos do XVIII Simpósio Brasileiro de Sistemas Colaborativos . SBC, 2023. p. 82-97.	Utilização de um <i>chatbot</i> como Disk Denúncia	<i>Chatbot</i> , Machine Learning	Aplicação de um <i>chatbot</i> para realização de denúncias de crimes.
8	MIRANDA, P. F. M.; SCHNEIDER, C. B. Vigilância e segurança pública: preconceitos e segregação social ampliados pela suposta neutralidade digital (Surveillance and public security: prejudices and social segregation widened	Relação entre tecnologia, segurança pública e vigilância e como IAs podem aumentar os casos de preconceito (ÉTICA)	O autor não cita nenhuma solução específica, mas reforça que IAs são reflexos dos seus criadores	Policiamento

	by the alleged digital neutrality). Emancipação, v. 20, n. 1, p. 16, 2020.			
9	INTELIGÊNCIA ARTIFICIAL, ALGORITMOS E POLICIAMENTO PREDITIVO NO PODER PÚBLICO FEDERAL BRASILEIRO. [s.l: s.n.]. Disponível em: < https://bdm.unb.br/bitstream/10483/24565/1/2019_MarcelleMartinsLemes_tcc.pdf >. Acesso em: 8 dez. 2023.	Utilização de big datas e inteligência artificial na segurança pública e implementação de um sistema “black box”	CCTV, Black boxes em IAs	Técnicas preditivas em CCTV
10	CHAUHAN, Aditi. AI For Smart Policing . Disponível em: < https://www.legalserviceindia.com/legal/article-7477-ai-for-smart-policing.html >.	Utilização de inteligência artificial para policiamento inteligente.	Predição por meio de análise, Machine Learning	Policiamento preditivo, identificação de criminosos, praticidade documental, monitoramento dos policiais.
11	AI Video Enhancement How Will AI Enhance Surveillance Video Quality. Disponível em: < https://www.any-video-converter.com/enhancer-ai/can-surveillance-video-be-ai-enhanced.html >. Acesso em: 8 dez. 2023.	Utilização de inteligência artificial em câmeras de vigilância	Upscaling, CCTV	Melhora na qualidade das imagens captadas pelas câmeras.
12	MOLINA-CABELLO, M. et al: FOREGROUND OBJECT DETECTION ENHANCEMENT Foreground object detection enhancement by adaptive super resolution for video surveillance. [s.l: s.n.]. Disponível em: < https://riuma.uma.es/xmlui/bitstream/handle/10630/18348/BMVC_2019_resize.pdf?sequence=1&isAllowed=y >. Acesso em: 8 dez. 2023.	Utilização de upscaling em câmeras de vigilância	Super Resolução(Upscaling)	Aprimoramento na detecção de objetos em primeiro plano utilizando Super Resolução
13	MOLEIRINHO, P. M. S. E.	Avaliação de aplicação de	reconhecimento	Melhoria no geral

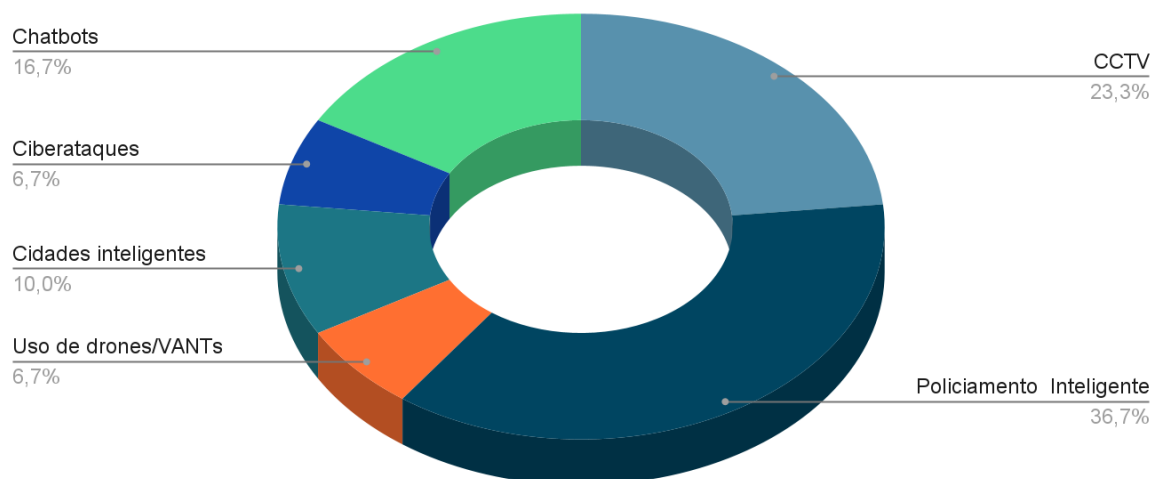
	Aplicação da inteligência artificial ao serviço da função policial. comum.rcaap.pt, 2021.	Tecnologias em forças policiais	o facial, análise de dados, previsão de crimes, detecção de anomalias em sistemas de segurança	das operações policiais
14	AL-AYROT, A.; SPARKMAN, J.; CONTRACTOR, U. Up-sampling low resolution surveillance feeds using GANs. [s.l: s.n.]. Disponível em: < http://cs230.stanford.edu/projects_winter_2021/reports/70759257.pdf >. Acesso em: 8 dez. 2023.	Melhoramento de imagens captadas por câmeras de segurança	Generative adversarial network (GANs), Super resolution Generative adversarial network (SRGANs)	Aprimoramento da qualidade de imagens captadas por câmeras de vigilância
15	ARAUJO, V. S. DE; ZULLO, B. A.; TORRES, M. 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, 1 set. 2020.	Propõe a analisar os riscos do uso de IAs e outras tecnologias para a sociedade	Machine learning, <i>chatbots</i>	Aplicações em big datas
16	JUNIOR, I. O.; DOS SANTOS, F. C. C. 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. <i>Brazilian Journal of Technology</i> , v. 5, n. 1, p. 030–062, 31 mar. 2022.	Utilização da inteligência artificial e do policiamento preditivo para o enfrentamento aos crimes violentos contra o patrimônio com emprego de explosivos pela Polícia Militar do Paraná.	Big Data, Machine Learning, Redes Neurais Artificiais	Aplicação para melhorar o monitoramento na polícia
17	FELDSTEIN, S. The Global Expansion of AI Surveillance. Disponível em:	O documento discute as diferentes técnicas de vigilância de IA usadas pelos governos em todo o mundo e como elas estão sendo	Cidades Inteligentes, Reconhecimento Facial e	

	< https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847 >	implantadas para alcançar objetivos políticos específicos.	Policimento Inteligente	
18	LAW ENFORCEMENT CHATBOTS CASE STUDY: 4. [s.l.: s.n.]. Disponível em: < https://aiethics.princeton.edu/wp-content/uploads/sites/587/2018/10/Princeton-AI-Ethics-Case-Study-4.pdf >.	Utilização do <i>Chatbot</i> JEREMY para identificação de cibercriminosos	<i>Chatbots</i>	Identificação de cibercriminosos utilizando PLN para aprender como eles se comunicam nos seus chats e fóruns.
19	CAMPBELL, Bill. How AI can help law enforcement agencies solve crimes faster. Disponível em: < https://www.police1.com/police-products/police-technology/articles/how-ai-can-help-law-enforcement-agencies-solve-crimes-faster-xg3GdkdLJnzcXVQ3/ >.	Como a utilização de IA pode ajudar na investigação e resolução de crimes	Assistente de IA para Real-Time Intelligence Center (RTIC).	
20	ZLATE, N. Chatbots, Future Undercover Investigators in the Criminal Process in the Artificial Intelligence Era? [s.d.].	Utilização de IA para investigações	<i>Chatbots</i> , Tecnologias de Reconhecimento Facial	Ajudar na identificação de criminosos e vítimas, mantendo uma conversa.
21	QIU, Xiaoying. Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks IEEE Journals & Magazine IEEE Xplore. Disponível em: < https://ieeexplore.ieee.org/document/8917569 >. Acesso em: 8 dez. 2023.	Utilização de IA para a proteção de dispositivos wireless	Deep learning, machine learning e redes neurais	Promover melhor segurança a dispositivos wireless por meio de autenticação via IA
22	Kumar, Rahul & Sajid, Mohammad & Gupta, Suneet & Haidri, Raza. (2022). Artificial Intelligence and Blockchain Technologies for Smart City. 10.1002/9781119816096.ch15.	Aplicação de IAs e blockchain em cidades inteligentes	Não especificado	Diferentes áreas de aplicação para melhorar cidades inteligentes como veículos, redução de esforço humano, entre outros

A partir da Tabela 1, nota-se que o conceito de SP utilizado vai além da segurança usualmente observada no dia a dia da população. Há trabalhos selecionados que tratam sobre cibersegurança, *chatbots* para auxiliar em denúncias, IA para maior rapidez nos processos de investigações criminais, entre outros. O presente trabalho busca trazer um panorama geral acerca dos mais diversos aspectos relacionados à segurança.

Figura 5: Principais aplicações identificadas

Porcentagem de aplicações



Fonte: Autores (2023).

A figura 5 foi criada a partir do material coletado do Quadro 4, aproveitando dos motores de busca anteriormente citados e os critérios de inclusão e exclusão. Para a coleta desses dados, foram utilizadas *strings* do Quadro 1. Entre todos os trabalhos encontrados, os seis temas que mais se destacaram no tema “utilização de IA na segurança pública” foram: Policiamento inteligente, circuito fechado de televisão(CCTV), ciberataques, cidades inteligentes, uso de drones/VANTs e *Chatbots*.

A partir desses temas levantados, foi decidido que seriam realizadas buscas a fim de obter a quantidade total de trabalhos que uniam os temas previamente expostos com segurança pública. Os resultados desta pesquisa são evidenciados no

tópico 5.1.

5.1. Busca do número total de trabalhos

Visando responder a questão primária da presente RSL, “Quais são as principais aplicações de IA na SP?”, utilizamos os seis principais temas previamente levantados, em *strings* semelhantes, as quais estão definidas no Quadro 2. Os resultados obtidos são expostos a seguir.

Ao realizar buscas buscando pelo termo “*smart policing*” e relacionados, foi retornado um total de 827 trabalhos, sendo 639(77.26%) em inglês e 188(22.74%) em português.

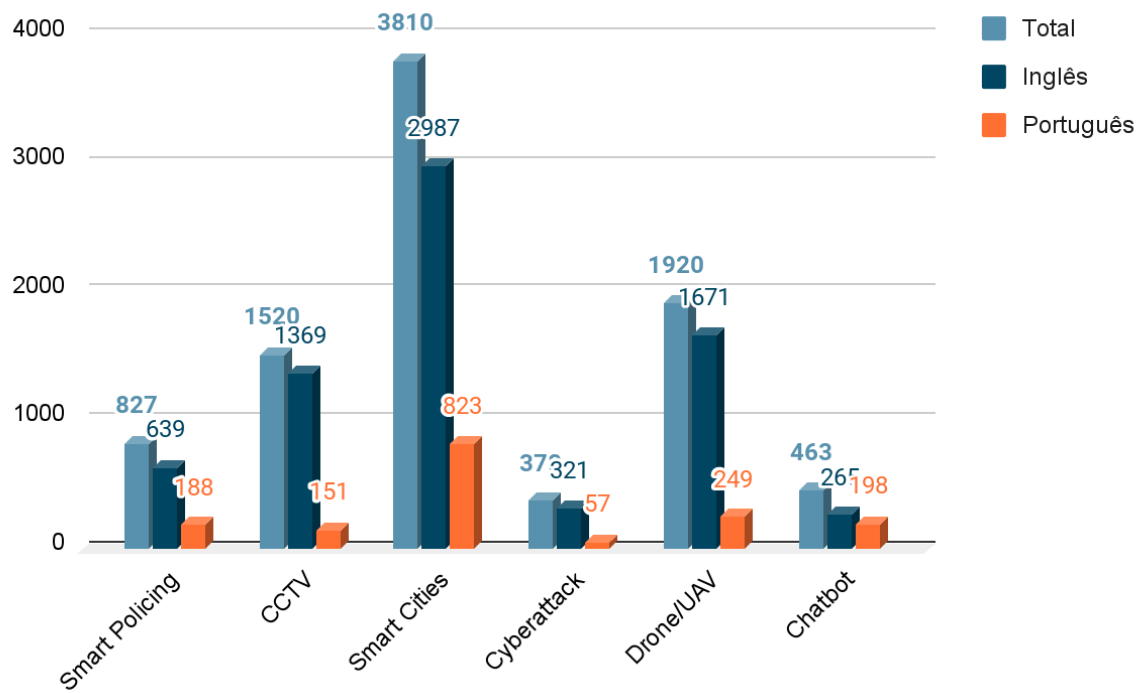
Para o termo “CCTV” foram retornados 1520 trabalhos no total, entre eles 1369(90.06%) em inglês e 151(9.94%) em português.

Em seguida, buscando pelas variações do termo “smart cities”, foram encontrados 3180 trabalhos. Destes, 2987(78.39%) em inglês e 823 (21.60%) em português.

Dando sequência nas buscas, ao pesquisar pelo termo “Cyberattack” e também “Ciberataque”, a pesquisa retornou 378 trabalhos, sendo 321(84.92%) em língua inglesa e 57(15,08%) em língua portuguesa.

Posteriormente, ao buscar por “drones” e termos relacionados, foram encontrados 1920 trabalhos, sendo 1671(87.0%) em inglês e 249(13.0%) em português.

Por fim, pesquisando pelo termo “*chatbot*”, foi obtido um retorno total 463 trabalhos, 265(57,23%) em língua inglesa e 198(42,77%) em língua portuguesa.

Figura 6: Quantidade de trabalhos por *string*

Fonte: Autores (2023)

6. DISCUSSÃO DOS PRINCIPAIS TERMOS E RESULTADOS

A partir da quantidade de trabalhos retornados, destaca-se uma predominância de trabalhos na língua inglesa. Tal fato justifica-se por alguns fatores:

- A língua inglesa é amplamente aceita na comunidade científica internacional como língua a língua franca;
- Maior reconhecimento e credibilidade;
- Facilidade de colaboração;
- entre outros.

Contudo, apesar dessas barreiras, as buscas por “*chatbot*” retornaram quantidades próximas de trabalhos em inglês e português. Demonstrando, assim, grande interesse da comunidade científica brasileira no assunto.

6.1 *Smart policing*

A integração da inteligência artificial (IA) no policiamento inteligente tem se destacado como uma abordagem inovadora e eficaz para melhorar a segurança pública. De acordo com Chauhan (2023), o policiamento inteligente enfatiza a prevenção de crimes e incentiva o fortalecimento da base de evidências da polícia. O policiamento inteligente concentra-se na utilização eficiente de dados e análises, aprimorando o monitoramento. De acordo com Junior (2021), a aplicação de IAs nesse contexto pode se dar seguinte maneira:

“A IA emerge como ferramenta capaz de potencializar a análise de grandes volumes de dados estruturados e não estruturados armazenados em repositórios institucionais como o sistema BOU (Boletim de Ocorrência Unificado), pelos relatórios de atendimento de ocorrência produzidos pela unidade antibombas do BOPE, pelos relatórios do sistema de inteligência da PMPR, combinados com outras bases de dados governamentais (saúde, educação, economia) e ainda aqueles oriundos da conectividade entre dispositivos capazes de produzir dados”

Em relação ao policiamento inteligente, a IA também desempenha um papel crucial na otimização da investigação criminal. Ferramentas de análise de dados podem identificar conexões entre incidentes aparentemente isolados e fornecer informações cruciais de diversas fontes, incluindo polícia, agências federais ou outros serviços comunitários, oferecendo, assim, as informações mais precisas e

atualizadas disponíveis, facilitando a resolução de casos complexos (CAMPBELL, 2023).

Outra vantagem expressiva da utilização do policiamento inteligente encontrada nos trabalhos, foi o policiamento preditivo. Neste tipo de policiamento, a partir de uma análise de dados e histórico de acontecimentos, torna-se possível fornecer à polícia previsões sobre onde e quando as patrulhas policiais podem atuar ou manter a segurança, a fim de ter a melhor chance de dissuadir ou prevenir crimes potenciais (CHAUHAN, 2022). O autor Moleirinho(2020) conclui seu artigo da seguinte maneira:

“As Tecnologias de Informação e Comunicação têm vindo a ser paulatina e transversalmente adotadas pela sociedade, em geral e pelas Forças e Serviços de Segurança, em particular. Pretende-se alavancar a atividade operacional com base na proatividade, na preditividade e nos critérios de boa gestão. Este admirável mundo novo tem proporcionado inegáveis vantagens numa ótica de capacidades de comando e controle, na gestão e balanceamento de recursos e na eficácia da detecção, no controle e na erradicação da criminalidade. Contudo, considerando as capacidades de recolha e de análise massiva de dados, mantêm-se em aceso debate e escrutínio a sua utilização generalizada, em vista do cumprimento dos princípios constitucionais da liberdade, da segurança e da privacidade.”

6.2 CCTV

Os CCTVs tradicionais têm limitações na interpretação de dados brutos. Todavia, com a introdução da IA, esses sistemas passam a analisar e entender de maneira mais eficiente o que está acontecendo em tempo real. Conforme estabelecido por Kruegle (2011):

“Em uma abordagem automatizada, a tecnologia de CCTV das cidades operam de maneira eficaz e confiável em um contexto mais amplo, fortalecendo o controle de tráfego, monitoramento técnico para proteção pública, melhora no tempo e na capacidade de resposta, reduzindo os custos relacionados a crimes e minimizando o tempo de investigação para aprimorar a capacidade de serviços de emergência em incidentes, catástrofes naturais e insurgências.”

Além disso, outras utilizações de IA para CCTV foram encontradas, como:

- **Reconhecimento facial:** Conforme definido por Feldstein (2019),

“Reconhecimento facial é uma tecnologia biométrica que utiliza câmeras, tanto de vídeo quanto de imagens estáticas, para comparar imagens armazenadas ou em tempo real de indivíduos com imagens de um banco de dados.” O potencial das tecnologias de reconhecimento facial utilizadas para SP é vasto. Bien (2023) exemplifica que quando conectado a um banco de dados com históricos criminais, CCTV é capaz de “monitorar indivíduos com condenações anteriores por atos relacionados a crimes em locais públicos, como perturbação da ordem pública, furto e roubo de propriedades em estações de trem e ônibus.”;

- **Upscaling:** Aliado à questão de vigilância por câmeras de segurança, também é possível citar as tecnologias de melhoramento de imagens, as quais podem ser utilizadas para auxiliar na identificação de objetos, rostos, placas de automóveis, entre outros, melhorando a imagem capturada, quando a mesma não se encontra suficientemente nítida. Um exemplo dessa tecnologia é o software *AVCLabs Video Enhancer AI* da empresa AVC e as demonstradas no trabalho proposto por Al-Ayrot, Sparkman, Contractor (2019). Outro trabalho encontrado propõe “uma metodologia para a melhorar a detecção de objetos em primeiro plano em uma sequência de vídeo” (MOLINA-CABELLO, 2019). Tal metodologia ajudou a melhorar o tempo de processamento de todas as *CPUs*, bem como a redução na utilização da memória. Vantagens bastante expressivas, principalmente para equipamentos de baixo custo.

6.3 Smart cities

De acordo com a Carta Brasileira para cidades inteligentes (2020) as cidades inteligentes buscam várias formas de aumentar a eficiência das ações feitas no seu território, dentre estas, as voltadas à segurança pública. Por ser um conceito mais amplo, cidades inteligentes abrangem inúmeras tecnologias, como IoT, CCTV, *blockchain*, entre outros. Tal abrangência também justifica a quantidade expressiva de trabalhos encontrados, sendo, dos principais temas discutidos, o que retornou o maior número de trabalhos.

O autor Kumar (2022) expõe como a inteligência artificial, combinada com outras tecnologias, têm sido eficiente:

“Especialmente, a rápida aceitação das tecnologias de Inteligência Artificial (IA) e blockchain tem conduzido a um paradigma que está se deslocando para uma nova dimensão chamada ecossistema digital para cidades inteligentes. Um grande número de aplicações de IA e blockchain garante soluções para desafios em campos que variam de serviços financeiros e gestão de ameaças a criptomoedas, e de serviços sociais e públicos à Internet das Coisas (IoT).”

Dentre as várias tecnologias presentes em cidades, é possível extrair as de IA e relacioná-las com a aplicação e gestão de SP. Nos trabalhos selecionados, as principais vantagens da utilização de IA na SP em cidades inteligentes foram:

- Vigilância por vídeo;
- Gestão de tráfego e mobilidade;
- Análise preditiva;
- Identificação de padrões comportamentais;
- Drones para monitoramento;

6.4 Cyberattacks

A cibersegurança é um tópico muito presente quando se refere à sociedade moderna. O grande fluxo de informações constantes gera preocupações acerca da segurança dos dados e invasão de dispositivos. Seguindo essa linha, um dos trabalhos, nomeado como *“Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks”*, ou Autenticação de segurança baseada em inteligência artificial: Aplicações nas redes de multimídia sem fio em português, menciona uma estratégia eficaz para melhoria da cibersegurança.

Nesse caso, a ideia é proteger dispositivos wireless com aplicações em IOT como assistentes, travas eletrônicas, entre outros. Para que esse processo seja possível, a autora do texto Xiaoying Qiu (2019) descreve:

“Geralmente, técnicas de autenticação e controle de acesso são consideradas como mecanismos-chave e designs críticos para o paradigma multimídia, uma vez que atacantes adversários necessitam dos requisitos de acesso aos recursos multimídia. Essas técnicas asseguram comunicações legítimas ao confirmar as identidades de todos os usuários e seu acesso à rede autorizada. No entanto, a particularidade de um grande número de dispositivos multimídia apresenta novos desafios de design para

configurações de segurança. Explicitamente, dispositivos multimídia que reivindicam transmissões de baixa latência podem não oferecer suporte a métodos de autenticação que exigem alta carga computacional, e os sensores enormes contidos em um sistema multimídia sem fio requerem custos computacionais leves para garantir seu desempenho de comunicação. Portanto, para se defender contra ameaças de ataques em redes multimídia sem fio, este artigo se concentra nos desafios enfrentados por esquemas de autenticação tradicionais e propõe novos métodos de aprimoramento de segurança”.

A ideia de criar um autenticador que aprende os padrões dos atacantes e dos usuários comuns não é só uma excelente ideia num ponto de vista de segurança, mas também na carga de utilização dos hardwares e na velocidade que essa ação é acionada.

Figura 7: comparação dos resultados

Parameter	Intelligence based LPLA scheme	Key based cryptography scheme
Key management and transmission	No	Yes
Channel estimation	Yes	Yes
Feature selection	No	Yes
Pricy amplification	No	Yes
Adaptability	Yes	No
Latency	Low	High
Link	Physical layer	Upper layer
Time complexity of n authentications	$O(1)$	$O(n)$

Fonte: Xiaoying Qiu (2019)

A Figura 7 demonstra algumas das vantagens em comparação a criptografia comum por chaves, que são mais comumente aplicadas:

- A primeira linha mostra como a inteligência artificial consegue autenticar sem o uso de chaves, as quais podem ser invadidas e quebradas via rede;
- Mostra também na quinta linha que a IA é mais adaptável a diferentes

situações de risco;

- Mostra na sexta linha que a latência é significativamente menor.

Outro trabalho, por Zeadally (2020), ressalta a importância da utilização de IA na cibersegurança. "Com o aumento da velocidade e sofisticação dos ciberataques, IA tem se tornado uma tecnologia indispensável na cibersegurança". Sua aplicação traz benefícios como: detecção e mitigação de ameaças aprimoradas; adaptabilidade a ameaças em evolução, automação de processos de segurança, entre outros.

6.5 Drone/UAV

A utilização de drones ou veículos aéreos não tripulados pode se estender para vários campos além da segurança pública: Utilização militar, doméstica e entretenimento são algumas das aplicações fora da segurança pública, e não necessariamente utilizadas com IA.

Spanaki (2021), propõe a utilização de drones e UAVs para monitoramento de lavouras. A ideia é utilizar "enxames" de drones que vigiam as plantações, detectam problemas visuais e instruem outros drones no enxame para corrigir esses problemas, caso possível.

O texto em questão cita esse exemplo na segurança alimentícia, mas também faz um breve comparativo com a segurança pessoal. Essa aplicação pode ajudar trabalhadores em fazendas a se arrisquem menos ou até ser replicada para cidades inteligentes.

Outro trabalho, por Thakur (2021), evidencia que UAVs podem ser usados para dar suporte aos guardas de segurança, rastreando indivíduos, e também para oferecer proteção a quaisquer ameaças, localizando e identificando criminosos por meio de reconhecimento facial.

6.6 Chatbot

A incorporação de *chatbots* na segurança pública tem se mostrado uma estratégia eficaz para melhorar a comunicação, fornecer informações em tempo real e aprimorar a eficiência operacional.

Os robôs são uma solução oportuna para uma geração que prefere mensagens de texto aos meios tradicionais de comunicação (CIECHANOWSKI et al., 2018). Seguindo essa linha de pensamento, o trabalho de De Ferran e Motta (2023) buscou desenvolver um *chatbot* como *disk* denúncia. Os resultados mostraram que DORA, o *chatbot* desenvolvido, além de mais eficaz, era capaz de identificar e reconhecer sub-denúncias.

Outros trabalhos também identificaram que, pela eficiência no atendimento e velocidade das respostas, a utilização de *chatbots* para esse quesito também “pode melhorar a percepção, a confiança e a satisfação das vítimas por meio de sua comunicação e ao manter as vítimas informadas sobre a investigação.” (RTI, 2023). Como também afirma Zlate (2022):

“É inegável que os chatbots têm o potencial de ampliar o acesso à justiça (por exemplo, auxiliando constantemente vítimas de crimes a conhecerem seus direitos acessíveis e recursos legais, a redigir diversos atos), aumentar a participação da comunidade e reduzir custos ao aprimorar a eficiência, graças à capacidade de processar automaticamente uma grande quantidade de dados e realizar tarefas.”

Além disso, outra vantagem foi identificada no estudo de caso realizado pela Universidade de Princeton (2017), na qual utilizaram o *chatbot* JEREMY para análise de comportamento de cibercriminosos e também interrogá-los.

6.7. A Ética nos trabalhos

Ao realizar a busca dos trabalhos encontramos trabalhos que não respondiam nossa questão primária, mas sim a questão secundária: Quais as principais problemáticas das aplicações e ferramentas de IA na SP?

Entre os diversos tópicos estudados, alguns se destacam por estabelecer uma preocupação extra quanto ao tema. A preocupação com o futuro é justificada e, de acordo com a autora Schneider (2020), diversos questionamentos são criados: “Quem alimenta o sistema de dados? Que tipo de informação é armazenada? Quais são as suas fontes? Quais as consequências da utilização desse mecanismo na elaboração de sistemas de vigilância? O que acontece se delegarmos o poder aos criadores dessas tecnologias de segurança?”. Como também enfatizado por Sousa

(2019), “É importante enfatizar que a IA é usada conforme foi projetada; assim, se não houver controle e regulamentação adequados, comportamentos humanos indesejados podem ser replicados pela máquina, como preconceito e discriminação”.

A autora cita também sobre como as pessoas que são marcadas digitalmente estão fadadas a se tornarem “refugos digitais”. As marcas digitais dificilmente serão completamente perdidas e, por mais das ações tomadas por algoritmos e inteligências dependerem dos seus criadores, não é possível prever como um sistema inteligente irá agir ao estar em uma situação como essa. No mesmo artigo, Schneider cita uma pesquisa realizada pelo *Human Rights Data Analysis Group*:

“Outro programa utilizado nos Estados Unidos, o PredPol, é um algoritmo que afirma prever quando e onde ocorrerão os crimes. O objetivo era ajudar a reduzir o viés humano no policiamento. Porém, a mundialmente conhecida organização sem fins lucrativos Human Rights Data Analysis Group (LUM, 2016) descobriu que o programa pode direcionar, injustamente, a polícia para certos bairros. Quando os pesquisadores efetuaram a simulação, o programa enviou policiais a bairros com maior proporção de pessoas pertencentes a minorias raciais, independentemente da taxa de criminalidade ali existente”

Outro dos artigos aponta preocupações parecidas: A falta de transparência das IAs. Araújo (2020), cita: “Uma característica problemática do processo decisório por meio de algoritmos baseados em machine learning é a da sua falta de transparência. A chamada “opacidade” do algoritmo é um ponto que já tem sido objeto de análise e debates”. Tal comentário exemplifica como a falta de ações sensíveis por parte das IAs também descredibiliza a democracia. O mesmo autor complementa: “Ações policiais concretas e decisões judiciais em âmbito criminal baseadas em processos cognitivos algorítmicos com vieses discriminatórios ofendem a dignidade da pessoa humana, o direito de igualdade e a liberdade do cidadão”.

A autora Lemes (2019) trata a visão do tema da seguinte maneira: “Diante de uma visão ampla, entretanto, a aproximação maior se dá com a sociedade de controle, sendo possível verificar elementos da sociedade disciplinar sobretudo nas fronteiras da sociedade liberal, cada qual produzindo efeitos subjetivos diferentes.” Esse comentário congloba as referências citadas: O medo de ser controlado.

Entre os termos que caracterizam a quebra de ética encontradas nos textos inclui-se:

- Discriminação (racial, social e geográfica);
- Invasão de privacidade;
- Direito administrativo à uma máquina;
- Falta de transparência nas decisões;
- Parcialidade nas decisões;
- Disseminação de *fake news*;
- Segregação líquida;
- Plano panóptico (vigilância constante).

Conclui-se que a utilização da IA na segurança pública abre diversas discussões. Não é possível compreender totalmente quais os riscos e vantagens, pois a utilização de IA está em constante evolução, mas muitos deles estão sendo previstos. A decisão de como identificar, expor e regulamentar as possíveis quebras de ética cabe aos órgãos de segurança.

7. CONCLUSÃO

Neste trabalho foi buscado trazer o estado da arte da pesquisa sobre IA na SP, bem como pontuar suas principais utilizações e também as problemáticas que circundam o tema. a investigação abrangente do estado da arte da inteligência artificial na segurança pública revelou avanços notáveis e uma ampla gama de aplicações promissoras.

O panorama atual demonstra que a IA desempenha um papel crucial na melhoria da eficiência operacional, prevenção de crimes e resposta a emergências. A utilização de algoritmos avançados de aprendizado de máquina em sistemas de vigilância, análise de dados e reconhecimento de padrões tem mostrado potencial para transformar positivamente a abordagem das forças policiais.

Contudo, é imperativo reconhecer as problemáticas que envolvem a integração da IA na segurança pública. Questões éticas, como a privacidade e a possibilidade de viés algorítmico, requerem uma atenção cuidadosa para garantir que essas tecnologias sejam implementadas de maneira ética e equitativa. A transparência nas práticas, a supervisão regulatória e a colaboração com a sociedade civil são essenciais para mitigar preocupações e garantir que a implementação da IA na segurança pública seja guiada por princípios éticos.

Ademais, conclui-se que a investigação realizada ressalta a importância da colaboração entre os especialistas em IA, órgãos legislativos, administrativos e judiciários. Buscar soluções capazes de facilitar as atividades humanas que ao mesmo tempo não invadam os direitos e privacidade humana é um grande desafio. Desafio esse que deve ser superado para que seja possível criar um futuro mais promissor a todos.

REFERÊNCIAS

ADAMOPOULOU, Eleni; MOUSSIADES, Lefteris. **Chatbots: History, technology, and applications. Machine Learning with Applications**, v. 2, p. 100006, 2020

AI Video Enhancement | How Will AI Enhance Surveillance Video Quality. Disponível em:

<<https://www.any-video-converter.com/enhancer-ai/can-surveillance-video-be-ai-enhanced.html>>. Acesso em: 8 dez. 2023.

ALLAM, Zaheer; DHUNNY, Zaynah A. **On big data, artificial intelligence and smart cities.** Cities, v. 89, p. 80-91, 2019.

AL-AYROT, A.; SPARKMAN, J.; CONTRACTOR, U. **Up-sampling low resolution surveillance feeds using GANs.** [s.l.: s.n.]. Disponível em: <http://cs230.stanford.edu/projects_winter_2021/reports/70759257.pdf>. Acesso em: 8 dez. 2023.

ARAUJO, V. S. DE; ZULLO, B. A.; TORRES, M. **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, 1 set. 2020.

Artificial intelligence bolsters public safety & security in smart cities | Security Magazine. Disponível em: <<https://www.securitymagazine.com/articles/99301-artificial-intelligence-bolsters-public-safety-and-security-in-smart-cities>>.

Artificial Intelligence-Based Security Authentication: Applications in Wireless Multimedia Networks | IEEE Journals & Magazine | IEEE Xplore. Disponível em: <<https://ieeexplore.ieee.org/document/8917569>>. Acesso em: 8 dez. 2023.

BERGLIND, N.; FADIA, A.; ISHERWOOD, T. **AI in government: Capturing the potential value** | McKinsey. Disponível em: <<https://www.mckinsey.com/industries/public-sector/our-insights/the-potential-value-of-ai-and-how-governments-could-look-to-capture-it>>.

BERTINO, E. et al. AI for Security and Security for AI. **Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy**, 26 abr. 2021.

BISLEV, Sven. **Globalization, state transformation, and public security.** International Political Science Review, v. 25, n. 3, p. 281-296, 2004.

BISWAS, Som S. **Role of chat gpt in public health.** Annals of biomedical engineering, v. 51, n. 5, p. 868-869, 2023.

BRASIL. **Carta brasileira para cidades inteligentes**. Brasília, DF: Ministério da Integração e do Desenvolvimento Regional, 2020.

BROOM, D. **AI: These are the biggest risks to businesses and how to manage them**. Disponível em:

<<https://www.weforum.org/agenda/2023/07/ai-biggest-risks-how-to-manage-them/>>.

BRUNDAGE, Miles et al. **The malicious use of artificial intelligence: Forecasting, prevention, and mitigation**. arXiv preprint arXiv:1802.07228, 2018.

CONG, V. T. et al. **APLICAÇÃO DE INTELIGÊNCIA ARTIFICIAL E DISPOSITIVOS DE MONITORAMENTO SOBRE PREVENÇÃO DE CRIMES DE DESORDEM PÚBLICA E CONDUTA DESORDEIRA**. Lex Humana (ISSN 2175-0947), v. 15, n. 1, p. 59–70, 30 jan. 2023.

CHATBOT. **Dicionário online de Cambridge**, 03 out. 2023. Disponível em: <<https://dictionary.cambridge.org/pt/dicionario/ingles/chatbot>>. Acesso em 03 out. 2023.

Chatbots for Law Enforcement – Enhanced Virtual Victim Assistant | RTI. Disponível em: <<https://www.rti.org/impact/chatbots-for-law-enforcement>>. Acesso em: 28 nov. 2023.

CHAUHAN, Aditi. **AI For Smart Policing**. Disponível em: <<https://www.legalserviceindia.com/legal/article-7477-ai-for-smart-policing.html>>.

CONFORTO, Edivandro Carlos; AMARAL, Daniel Capaldo; SILVA, SL da. **Roteiro para revisão bibliográfica sistemática: aplicação no desenvolvimento de produtos e gerenciamento de projetos**. Trabalho apresentado, v. 8, 2011.

CURRAN, D. Are you ready? This is all the data Facebook and Google have on you | Dylan Curran. Disponível em: <<https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy>>.

DE FERRAN, Cristianna M.; MOTTA, Claudia LR. Uso de Computação Cognitiva no Processo Semântico de um Atendente Virtual: Uma Aplicação na área da Segurança Pública. In: Anais Estendidos do XVIII Simpósio Brasileiro de Sistemas Colaborativos. SBC, 2023. p. 82-97.

EDU, Jide et al. **Exploring the security and privacy risks of chatbots in messaging services**. In: Proceedings of the 22nd ACM internet measurement conference. 2022. p. 581-588.

ELLINGRUD, K. et al. **Generative AI and the future of work in America** | McKinsey. Disponível em: <<https://www.mckinsey.com/mgi/our-research/generative-ai-and-the-future-of-work-in-america>>.

EUROPEAN COMMISSION. **Ethics guidelines for trustworthy AI | Shaping Europe's**

digital future. Disponível em:
<<https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai>>.

EUROPEAN PARLIAMENT, Directorate-General for Parliamentary Research Services, Fox-Skelly J, Bird E, Jenner N, Winfield A, Weitkamp E, Larbey R. **The ethics of artificial intelligence: issues and initiatives.** European Parliament; 2020. Available from: doi/10.2861/6644

FELDSTEIN, S. **The Global Expansion of AI Surveillance.** Disponível em:
<<https://carnegieendowment.org/2019/09/17/global-expansion-of-ai-surveillance-pub-79847>>

FIRAT, Mehmet. **How chat GPT can transform autodidactic experiences and open education.** Department of Distance Education, Open Education Faculty, Anadolu Unive, 2023.

GARCIA, A. C. **Ética e Inteligência Artificial.** Computação Brasil, n. 43, p. 14–22, 16 nov. 2020.

GIL, A. C. **Como elaborar projetos de pesquisa.** São Paulo: Atlas, 2002.. — Maurício Façanha. Disponível em:
<<https://docentes.ifrn.edu.br/mauriciofacanha/ensino-superior/redacao-cientifica/livros/gil-a.-c.-como-elaborar-projetos-de-pesquisa.-sao-paulo-atlas-2002./view>>.

GRAHAM, Stephen & Murakami Wood, David. (2003). **Digitizing Surveillance: Categorization, Space, Inequality.** Critical Social Policy - CRIT SOC POLICY. 23. 227-248. 10.1177/0261018303023002006.

GRYFO. **5 Aplicações de Inteligência Artificial em câmeras de segurança.** Disponível em:
<<https://gryfo-ai.medium.com/5-aplica%C3%A7%C3%B5es-de-intelig%C3%A2ncia-artificial-em-c%C3%A2meras-de-seguran%C3%A7a-7393ffc9bfd8>>. Acesso em: 28 nov. 2023.

HENMAN, P. (2020). **Improving public services using artificial intelligence: possibilities, pitfalls, governance.** Asia Pacific Journal of Public Administration, 1–13. doi:10.1080/23276665.2020.1816188

HENMAN, Paul. **Improving public services using artificial intelligence: possibilities, pitfalls, governance.** Asia Pacific Journal of Public Administration, v. 42, n. 4, p. 209-221, 2020.

CAMPBELL, Bill. **How AI can help law enforcement agencies solve crimes faster.** Disponível em:
<<https://www.police1.com/police-products/police-technology/articles/how-ai-can-help-law-enforcement-agencies-solve-crimes-faster-xg3GdkdLJnzcXVQ3/>>.

INTELIGÊNCIA ARTIFICIAL, ALGORITMOS E POLICIAMENTO PREDITIVO NO PODER

PÚBLICO FEDERAL BRASILEIRO. [s.l: s.n.]. Disponível em: <https://bdm.unb.br/bitstream/10483/24565/1/2019_MarcelleMartinsLemes_tcc.pdf>. Acesso em: 8 dez. 2023.

IWAZAKI, Anderson Yoshiaki. **Revisão Sistemática de Literatura**. Agosto, 2019. Slides em PDF. Disponível em: https://edisciplinas.usp.br/pluginfile.php/4932650/mod_resource/content/1/Systematic_Review__28_08.pdf. Acesso em 10 de ago. 2023.

JUNIOR, I. O.; DOS SANTOS, F. C. C. **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, 31 mar. 2022.

KITCHENHAM, B. **Procedures for Performing Systematic Reviews**. [s.l: s.n.]. Disponível em: <<https://www.inf.ufsc.br/~aldo.vw/kitchenham.pdf>>.

KRUEGLE, H. (2011). **CCTV surveillance: Video practices and technology**. Elsevier

Kumar, Rahul & Sajid, Mohammad & Gupta, Suneet & Haidri, Raza. (2022). **Artificial Intelligence and Blockchain Technologies for Smart City**. 10.1002/9781119816096.ch15.

LACOSTE, Yves. **Dicionário de Geografia Lisboa**, Teorema, 2005 [2003].

LAW ENFORCEMENT CHATBOTS CASE STUDY: 4. [s.l: s.n.]. Disponível em: <<https://aiethics.princeton.edu/wp-content/uploads/sites/587/2018/10/Princeton-AI-Ethics-Case-Study-4.pdf>>.

LIANG, Percy. **Learning executable semantic parsers for natural language understanding**. Communications of the ACM, v. 59, n. 9, p. 68-76, 2016.

LINDEBAUM, Dirk & Vesa, MIKKO & HOND, Frank. (2019). **Insights From “The Machine Stops ” to Better Understand Rational Assumptions in Algorithmic Decision Making and Its Implications for Organizations**. *Academy of Management Review*. 45. 10.5465/amr.2018.0181.

MAHESH, Batta. **Machine learning algorithms-a review**. *International Journal of Science and Research (IJSR)*. [Internet], v. 9, n. 1, p. 381-386, 2020.

MCDONALD, David D. **Natural language generation**. *Handbook of natural language processing*, v. 2, p. 121-144, 2010.

MIRANDA, P. F. M.; SCHNEIDER, C. B. **Vigilância e segurança pública: preconceitos e segregação social ampliados pela suposta neutralidade digital (Surveillance and public security: prejudices and social segregation widened by the alleged digital neutrality)**. *Emancipação*, v. 20, n. 1, p. 16, 2020.

MOLINA-CABELLO, M. et al.: **FOREGROUND OBJECT DETECTION ENHANCEMENT** *Foreground object detection enhancement by adaptive super resolution for video*

surveillance. [s.l: s.n.]. Disponível em: <https://riuma.uma.es/xmlui/bitstream/handle/10630/18348/BMVC_2019___resize.pdf?sequence=1&isAllowed=y>. Acesso em: 8 dez. 2023.

MOLEIRINHO, P. M. S. E. **Aplicação da inteligência artificial ao serviço da função policial.** comum.rcaap.pt, 2021.

MUSPRATT, A. **8 Surprising Examples of AI in Security.** Disponível em: <<https://www.intelligentautomation.network/business-intelligence/news/8-surprising-things-powered-by-ai-security>>. Acesso em: 28 nov. 2023.

OGAWA, Rodney & MALEN, Betty. (1991). **Towards Rigor in Reviews of Multivocal Literatures: Applying the Exploratory Case Study Method.** Review of Educational Research. 61. 265-286. 10.3102/00346543061003265.

PENNYCOOK, G. et al. **The Implied Truth Effect: Attaching Warnings to a Subset of Fake News Headlines Increases Perceived Accuracy of Headlines Without Warnings.** Management Science, v. 66, n. 11, 21 fev. 2020.

QUINTANA, Alexandra Diana Cicca. **Avaliação das técnicas de otimização para motores de busca.** 2012. Tese de Doutorado.

REVISTA NÚCLEO DE CRIMINOLOGIA VOLUME 07. [s.l: s.n.]. Disponível em: <http://www.atenas.edu.br/uniatenas/assets/files/magazines/Revista_Nucleo_Criminologia_07.pdf#page=129>. Acesso em 28 nov. 2023

RIGANO, C. **USING ARTIFICIAL INTELLIGENCE TO ADDRESS CRIMINAL JUSTICE NEEDS.** Disponível em: <<https://www.ojp.gov/pdffiles1/nij/252038.pdf>>.

ROTHER, E. T. **Revisão Sistemática x Revisão Narrativa.** Acta Paulista de Enfermagem, v. 20, n. 2, p. v–vi, jun. 2007.

RUZ, T. M. F. **Monitoramento Eletrônico de Logradouros Públicos - A Tecnologia a Serviço da Segurança Pública.** Revista Brasileira de Estudos de Segurança Pública, v. 1, n. 1, p. 1-5, 2008. Disponível em: <<https://doi.org/10.29377/rebsp.v1i1.72>>. Acesso em: 07 dez. 2023.

SAMOILI, Sofia et al. AI Watch. **Defining Artificial Intelligence. Towards an operational definition and taxonomy of artificial intelligence.** 2020.

SHAWAR, Bayan Abu; ATWELL, Eric. **Chatbots: are they really useful?.** Journal for Language Technology and Computational Linguistics, v. 22, n. 1, p. 29-49, 2007.

SHIDIK, GURUH FAJAR et al. **A systematic review of intelligence video surveillance: Trends, techniques, frameworks, and datasets.** IEEE Access, v. 7, p. 170457-170473, 2019.

SMITH, M., MILLER, S. **The ethical application of biometric facial recognition technology.** AI & Soc 37, 167–175 (2022). <https://doi.org/10.1007/s00146-021-01199-9>

SOUSA, W. G. DE et al. **How and where is artificial intelligence in the public sector going? A literature review and research agenda.** Government Information Quarterly, v. 36, n. 4, p. 101392, jul. 2019.

SPANAKI, K. et al. **Artificial intelligence and food security: swarm intelligence of AgriTech drones for smart AgriFood operations.** Production Planning & Control, p. 1–19, 25 fev. 2021.

ZLATE, N. Chatbots, Future Undercover Investigators in the Criminal Process in the Artificial Intelligence Era? [s.d.].

SCHAAL, S. **The Four “Pure” Learning Styles in Machine Learning.** Disponível em: <<https://towardsdatascience.com/the-four-pure-learning-styles-in-machine-learning-a6a1006b9396>>. Acesso em: 28 dez. 2023.

SURAMEERY, Nigar M. Shafiq; SHAKOR, Mohammed Y. **Use chat gpt to solve programming bugs.** International Journal of Information Technology & Computer Engineering (IJITC) ISSN: 2455-5290, v. 3, n. 01, p. 17-22, 2023.

TAVARES DE SOUZA, M.; DIAS DA SILVA, M.; DE CARVALHO, R. **Revisão integrativa: o que é e como fazer. Integrative review: what is it? How to do it?** Einstein, v. 8, n. 1, p. 102–108, 2010.

TEGA, I. **Sistema com IA faz reconhecimento facial em 0,2 segundo.** Disponível em: <<https://forbes.com.br/forbes-tech/2023/06/brandvoice-intelbras-sistema-com-ia-faz-reconhecimento-facial-em-02-segundo/>>. Acesso em: 28 nov. 2023.

TIPOS DE REVISÃO DE LITERATURA. [s.l.: s.n.]. Disponível em: <<https://www.fca.unesp.br/Home/Biblioteca/tipos-de-revisao-de-literatura.pdf>>.

THAKUR, N. et al. **Artificial Intelligence Techniques in Smart Cities Surveillance Using UAVs: A Survey.** p. 329–353, 1 jan. 2021.

UNESCO. Recomendação sobre a Ética da Inteligência Artificial. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000381137_por>. Acesso em: nov. 2023.

VEDOVA, Daiane. **O que é segurança pública.** Disponível em <<https://www.jusbrasil.com.br/artigos/o-que-e-seguranca-publica/586735267>>

WEBER, Max. **ECONOMIA E SOCIEDADE: Fundamentos da sociologia compreensiva,** UNB. São Paulo, 2004

What It Means When You Have “SSSS” on Your Boarding Pass. Disponível em: <<https://www.afar.com/magazine/ssss-on-your-boarding-pass-step-this-way#:~:text=Secure%20Flight%20is%20a%20risk>>. Acesso em: 28 nov. 2023.

XAVIER, C. F. M. C. S. **Sistema de cerca inteligente para ocorrências policiais em smart cities.** 2020. Trabalho de Conclusão de Curso (Graduação em Engenharia de Telecomunicações) – Escola de Engenharia, Universidade Federal Fluminense, Niterói,

2020.

YANG, Xin et al. **Concepts of artificial intelligence for computer-assisted drug discovery**. Chemical reviews, v. 119, n. 18, p. 10520-10594, 2019.

YIN, CHUAN TAO et al. **A literature survey on smart cities**. Sci. China Inf. Sci., v. 58, n. 10, p. 1-18, 2015

Z. KRUTILLA AND A. KOVARI, **"The origin and primary areas of application of natural language processing,"** 2022 IEEE 22nd International Symposium on Computational Intelligence and Informatics and 8th IEEE International Conference on Recent Achievements in Mechatronics, Automation, Computer Science and Robotics (CINTI-MACRo), Budapest, Hungary, 2022, pp. 000293-000298, doi: 10.1109/CINTI-MACRo57952.2022.10029432.

ZEADALLY, S. et al. **Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity**. IEEE Access, v. 8, p. 1–1, 2020.

ZUIDERWIJK, Anneke; CHEN, Yu-Che; SALEM, Fadi. **Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda**. Government Information Quarterly, v. 38, n. 3, p. 101577, 2021.