Cadernos do IUM

INTELIGÊNCIA ARTIFICIAL: ESTUDOS PIONEIROS EM CONTEXTO MILITAR

Coordenação de:
Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

IUM

Agosto 2024

INSTITUTO UNIVERSITÁRIO MILITAR

INTELIGÊNCIA ARTIFICIAL: ESTUDOS PIONEIROS EM CONTEXTO MILITAR

Coordenadora

Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

IUM – Centro de Investigação e Desenvolvimento (CIDIUM)
Agosto de 2024

Como citar esta publicação:

Esteves, A. C. C. S. M. (Coord.), (2024). *Inteligência Artificial: Estudos Pioneiros em Contexto Militar.* Cadernos do IUM, 60. Lisboa: Instituto Universitário Militar.

Diretor
Tenente-General Hermínio Teodoro Maio

Editora-chefe
Coronel Joana Isabel Azevedo do Carmo Canhoto Brás

Coordenadora Editorial
Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

Capa – Composição Gráfica
Tenente-coronel Ana Carina da Costa e Silva Martins Esteves
Imagem gerada por Inteligência Artificial em agosto de 2024

Secretariado
Assistente Técnica Gisela Cristina da Rocha Basílio

Propriedade e Edição
Instituto Universitário Militar
Rua de Pedrouços, 1449-027 Lisboa
Tel.: (+351) 213 002 100
Fax: (+351) 213 002 162
E-mail: cidium@ium.pt
https://cidium.ium.pt/site/index.php/pt/publicacoes/as-colecoes

Paginação, Pré-Impressão e Acabamento
What Colour Is This?
Rua Roy Campbell Lt 5 -4º B
1300-504 Lisboa
Tel.: (+351) 219 267 950
www.wcit.pt

ISBN: 978-989-35731-1-2
ISSN: 2183-2129
Depósito Legal: 541405/24
Tiragem: 90 exemplares

Nota do Editor:

Os textos/conteúdos do presente volume são da exclusiva responsabilidade dos seus autores.

iii

NOTA EDITORIAL

Estimados leitores,

Esta obra marca a primeira publicação dedicada exclusivamente à Inteligência Artificial (IA) no contexto militar, reunindo cinco estudos que refletem sobre a importância da sua integração estratégica.

Face à ausência de uma estratégia nacional para a IA na Defesa, o primeiro estudo sugere a criação de uma estrutura de governação que monitore e promova o desenvolvimento de IA no setor. O segundo estudo explora a liderança do conhecimento e a incorporação de tecnologias de IA nas Forças Armadas Portuguesas, propondo 17 recomendações para uma exploração mais eficiente destas tecnologias em operações militares.

O terceiro estudo investiga como a IA pode otimizar o processo de planeamento de operações da OTAN, especialmente nas Operações Especiais, ao automatizar tarefas analíticas complexas e integrar dados de várias fontes. No quarto estudo, a IA é analisada no contexto dos Sistemas de Informação Geográfica da Guarda Nacional Republicana, destacando o seu potencial para reforçar o policiamento preditivo e melhorar a gestão de recursos no combate ao crime.

Por fim, o quinto estudo examina a aplicação de IA na prevenção de sinistralidade rodoviária em Portugal, com destaque para o projeto MOPREVIS da Universidade de Évora. Este estudo identifica quatro linhas de orientação estratégica para maximizar a utilização de IA na prevenção de acidentes rodoviários e no alerta precoce.

Esta publicação pioneira oferece uma importante contribuição para o avanço da compreensão e implementação da IA no setor público, com um foco especial nas áreas da Segurança e Defesa. Destina-se a profissionais, académicos e decisores políticos que procuram explorar o potencial da IA para enfrentar os desafios e oportunidades no contexto militar e de segurança pública.

Desejo-lhe uma proveitosa leitura!

Ana Esteves
Tenente-coronel
Coordenadora editorial do CIDIUM

ÍNDICE

INTRODUÇÃO GERAL

Deslumbrada e detentora de super poderes é como qualquer pessoa se sente ao conseguir produzir com mais qualidade e maior rapidez, utilizando as facilidades da Inteligência artificial (IA). Não é só sensação, estudos demonstram que a qualidade aumenta entre 20% a 40% e a rapidez entre 37% e 25%, de acordo com Black (2023) e Noy e Zhang (2023), respetivamente. A tentação é grande assim como a dúvida. É seguro usar IA nas organizações? De que forma se deve usar a IA? O debate e os estudos têm-se densificado, motivados pela controvérsia e pela desconfiança. Efetivamente, não é obvio usar a IA de forma correta e para as tarefas certas, assim como também não é saber quando a IA é adequada ou não. Dá-se o paradoxo de as pessoas desconfiarem da IA em áreas onde ela pode contribuir com elevado valor, e confiar demasiado em áreas onde a IA não é competente (Candelon et al., 2023).

No contexto militar, estudos dos últimos cinco anos revelam que a IA está a ser cada vez mais integrada em aplicações militares em vários domínios, oferecendo um potencial significativo para revolucionar a guerra e melhorar as capacidades das Forças Armadas (Steff & Abbasi, 2020; Bitzinger & Raska, 2022). As suas aplicações incluem sistemas de armas automatizados, *drones*, guerra cibernética e eletrónica, análise de informações e apoio à tomada de decisões (Șușnea & Buță, 2021). Acrescem aplicações que vão desde os sistemas autónomos de defesa por satélite até à análise preditiva (Bokonda et al., 2020; Dagnaw & Endeshaw, 2019). Além disso, a IA está a ser utilizada para aprimorar a consciência situacional, os sistemas de alerta precoce e o planeamento operacional (Davis & Bracken, 2022) o reconhecimento de imagens, a análise de texto, os veículos autónomos, a automatização de processos robóticos e os sistemas de armas autónomos (Jayakumar et al., 2021).

Apesar do entusiasmo em torno da IA, existe um debate sobre o seu real impacto militar. Alguns especialistas acreditam que a IA irá transformar todos os aspetos da guerra, enquanto outros defendem que a tecnologia ainda está num estágio inicial e imaturo para ter um efeito decisivo no campo de batalha (Rickli & Mantellassi, 2023). Este contraste reflete a incerteza sobre as limitações e o potencial da IA em contextos de guerra. Um conceito emergente, o da inteligência aumentada, propõe uma sinergia entre humanos e máquinas como abordagem complementar (Sadiku et al., 2021).

À medida que a IA continua a evoluir, os países estão a torná-la uma componente central das suas estratégias militares, reconhecendo o impacto potencial desta tecnologia no equilíbrio estratégico global (Horowitz et al., 2020). No entanto, o desenvolvimento e a implementação da IA em operações militares levantam desafios significativos, desde questões éticas até à necessidade de criar mecanismos de confiança para evitar riscos imprevistos associados a esta corrida tecnológica (Rashid et al., 2023). A gestão eficaz desses riscos é crucial para garantir a estabilidade internacional.

Considerando todos os recentes desafios e a necessidade de pensar criticamente, a presente publicação revela-se essencial, constituindo-se como a primeira dedicada exclusivamente à análise da IA no contexto militar. Reúne cinco estudos de investigação realizados por alunos, auditores dos Cursos de Promoção a Oficial General e de Estado-Maior Conjunto, no âmbito dos seus trabalhos de final de curso, e tendem a contribuir para ampliar os tópicos de reflexão e o entendimento sobre o futuro da IA nas Forças Armadas.

A relevância destes estudos é amplamente respaldada por uma série de documentos estratégicos globais que destacam a crescente importância da Inteligência Artificial (IA) em vários campos, especialmente na defesa, segurança e saúde. O discurso de Putin sublinha a IA como um componente crucial para o futuro global, e o plano estratégico da China aponta para a ambição de ser líder mundial nessa tecnologia até 2030. A Ordem Executiva dos EUA n.º 13859 reafirma a centralidade da liderança americana na área, enquanto a OTAN e a OCDE destacam a aplicação da IA na defesa e segurança como um fator transformador. Mesmo Portugal, com sua Estratégia Nacional de IA, alinha-se com esses desenvolvimentos, embora ainda precise integrar mais explicitamente a IA no âmbito da Defesa.

Além disso, a relevância dos estudos é reforçada por documentos que evidenciam o papel estruturante da IA nas Forças Armadas. O Conceito Estratégico da OTAN aponta a IA como uma tecnologia essencial no contexto geopolítico global, com impacto direto na capacidade de combate, eficiência militar e na previsão de ações inimigas. O avanço de sistemas robóticos e a urgência de garantir o controle humano sobre tecnologias inteligentes são questões críticas, como indicado pela OTAN e pelos desafios evidenciados no conflito Rússia-Ucrânia.

Os estudos são também fundamentados pela Comissão Europeia, que aponta a transformação digital como um fator chave na evolução da segurança,

e pelas diretrizes do Parlamento Europeu, que estabelecem normas regulatórias para a IA. Tais diretrizes são fundamentais para a implementação de tecnologias emergentes nas operações militares e nas forças de segurança, como a Guarda Nacional Republicana (GNR), que já utiliza IA e sistemas de informação geográfica (SIG) no policiamento preditivo.

A sinistralidade rodoviária, também considerada um problema de saúde pública global pela OMS (2021), destaca-se como outra área crítica onde a IA tem se mostrado promissora. Com mais de 1,3 milhões de mortes anuais devidas a acidentes rodoviários, a adoção de tecnologias preditivas, como demonstrado por projetos da Universidade de Évora e da GNR, é um passo importante para melhorar a segurança nas estradas.

Essas questões levantam a urgência de integrar a IA em diversas esferas, desde a defesa à segurança pública, promovendo uma reflexão sobre como maximizar o impacto positivo dessas tecnologias, alinhando-as com as diretrizes globais e locais para um futuro mais seguro e eficiente.

O primeiro estudo "Inteligência Artificial: Contributos para uma Estratégia na Área da Defesa" destaca a importância estratégica da inteligência artificial (IA) para a Defesa Nacional para proporcionar vantagem decisória e operacional, tendo em conta o crescimento exponencial de dados. Apesar de avanços em iniciativas específicas, como na Marinha e no Exército, ainda não existe uma estratégia centralizada para a IA na Defesa, ao contrário de outros países da OTAN que já lideram nesse domínio. O estudo sugere a criação de uma estratégia específica para IA, acompanhada por uma estrutura centralizada no Ministério da Defesa Nacional, que seja capaz de coordenar e implementar projetos de IA de forma transversal. O trabalho oferece um diagnóstico sobre o estado atual da IA na Defesa em Portugal e apresenta um roteiro estratégico inspirado em práticas internacionais. A meta é alcançar autonomia estratégica em IA até 2032, alinhando o país aos padrões globais e reforçando sua posição na OTAN e na UE.

O segundo estudo "Aplicação das Tecnologias de Inteligência Artificial em Operações Militares" justifica a importância da IA como resposta à evolução tecnológica global, que combina *big data,* poder computacional e avanços em *machine learning*, desafios que têm impacto direto nas áreas de Segurança e Defesa. Essa evolução é ainda mais significativa considerando a escassez de recursos humanos nas Forças Armadas (FA) e a crescente complexidade tecnológica dos sistemas de armas. A IA surge como um elemento transformador,

potencializando a inteligência humana e oferecendo vantagens em previsão e atuação antecipada, especialmente em funções críticas como C2, inteligência e apoio logístico. As conclusões destacam a necessidade de desenvolver mecanismos de financiamento, capacitar recursos humanos, criar uma diretiva estratégica para IA e estabelecer parcerias com a academia e outras organizações. Além disso, propõe-se o fortalecimento de infraestruturas de dados e inovação para viabilizar a aplicação prática da IA em áreas prioritárias como manutenção preditiva, veículos autónomos e ciberespaço. É apresentado um conjunto de propostas validadas metodologicamente, direcionadas à melhoria da capacidade das FA no uso da IA até 2030. Tais propostas abrangem dimensões como organização, progresso tecnológico, adoção estratégica, inovação, gestão de dados e desenvolvimento de talentos, estabelecendo um roteiro claro para alcançar maturidade tecnológica e vantagem operacional no uso de IA em defesa.

No terceiro estudo "O Papel das Tecnologias de Inteligência Artificial na Adaptação das Capacidades Militares às Ameaças Modernas – Contributos para o seu Emprego" releva a IA para a modernização militar, destacando seu impacto transformador em operações militares. O exemplo do conflito Rússia-Ucrânia demonstra a sua aplicação prática na análise de grandes volumes de dados para gerar informações estratégicas em tempo real, na identificação de alvos e na defesa cibernética. Dada a crescente complexidade das ameaças modernas, a IA emerge como essencial para melhorar a eficiência dos sistemas de comando e controle, otimizando processos decisórios. Desta forma, é explorada a aplicação da IA no Planeamento Operacional da NATO, especialmente no contexto das Operações Especiais, com o intuito de aprimorar o processo SOCC-P2. A pesquisa analisa como a IA pode superar desafios como integração de informações, escassez de pessoal qualificado e limitações de tempo, através do uso de algoritmos avançados em processamento de linguagem natural, *machine learning*, visão computacional e sistemas especializados. Os contributos para o conhecimento incluem a identificação de ferramentas e técnicas específicas de IA com potencial de otimização no contexto militar. Além disso, destaca-se a importância de soluções adaptadas à realidade das Forças Armadas Portuguesas, considerando restrições financeiras e tecnológicas.

O quarto estudo "Aplicação da Inteligência Artificial ao Serviço da Função Policia" examina como a IA, está a integrar a componente operacional da Guarda Nacional Republicana, com potencial para aumentar a eficiência no combate à criminalidade, ao melhorar capacidades de comando e controlo, otimizar recursos

e aperfeiçoar a análise e predição de riscos. Ao mesmo tempo, a sua aplicação enfrenta desafios legais, éticos e operacionais relacionados com a privacidade e direitos fundamentais. É analisada a integração da IA nos Sistemas de Informação Geográfica (SIG) na GNR, abordando suas implicações para a construção de mapas de risco, análise preditiva de criminalidade e alocação eficiente de recursos. A pesquisa destaca benefícios, como maior precisão na avaliação de riscos, monitoramento aprimorado e geração de indicadores preditivos, ao mesmo tempo em que ressalta a necessidade de conformidade com princípios legais e éticos, como anonimização de dados e mecanismos de fiscalização. O estudo evidencia o impacto transformador da IA para refinar preditividade, melhorar o balanceamento de recursos e aprimorar a tomada de decisões, propondo caminhos para sua adoção sustentável e eficaz, em alinhamento com as necessidades operacionais e princípios constitucionais.

Por fim, o quinto estudo "Prevenção e Alerta da Sinistralidade Rodoviária com o Contributo da Inteligência Artificial" aborda a IA como uma solução promissora para a prevenção e mitigação de sinistros rodoviários, especialmente através de modelos preditivos que melhoram a tomada de decisão e a gestão de emergências. O projeto MOPREVIS, desenvolvido em Portugal, destaca-se como exemplo de aplicação prática dessa tecnologia, mostrando potencial para reduzir a sinistralidade através de ferramentas digitais de apoio em tempo real. Os contributos para o conhecimento incluem a sistematização de estratégias para melhorar a qualidade, automação e diversificação de dados, e fomentar a colaboração interinstitucional. O estudo enfatiza a necessidade de rigor na recolha e gestão de dados, bem como no desenvolvimento de novas variáveis para refinar as análises preditivas. O MOPREVIS é apresentado como um modelo de elevada relevância, com potencial para transformar o planejamento operacional e a alocação de recursos da GNR, aumentando a eficácia na prevenção de acidentes rodoviários e na proteção de vidas.

Em conjunto, os estudos exploram a aplicação da Inteligência Artificial em áreas estratégicas como Defesa Nacional, operações militares, policiamento e prevenção de acidentes rodoviários. Todos destacam o potencial da IA, especialmente do *machine learning* e da análise de grandes volumes de dados, para otimizar operações, melhorar a eficiência e reduzir recursos e tempo. Além disso, apontam a necessidade de desenvolver estratégias formais e estruturas de governança, promovendo a cooperação entre entidades para maximizar os benefícios da IA em contextos de segurança e defesa.

Os cinco estudos apresentados destacam-se pela sua relevância na abordagem de questões críticas de segurança, gestão e inovação, com foco na aplicação de tecnologias emergentes como a inteligência artificial. Cada um, à sua maneira, evidencia como soluções tecnológicas e metodologias multidisciplinares podem ser integradas em contextos operacionais complexos, contribuindo para avanços significativos em áreas prioritárias como a gestão de riscos criminais, a prevenção da sinistralidade rodoviária e a eficiência das forças de segurança.

Estes trabalhos não só aprofundam o conhecimento científico, mas também promovem a transição para práticas mais sustentáveis, éticas e proativas, alinhadas com os desafios contemporâneos. Ao cruzar o rigor técnico com a preocupação com os direitos fundamentais e os valores éticos, oferecem contributos valiosos para a evolução das instituições e o fortalecimento da segurança pública. Assim, os resultados destes estudos não apenas orientam políticas e práticas imediatas, mas também lançam bases sólidas para o desenvolvimento futuro de estratégias que conciliem inovação, eficiência e responsabilidade social, fundamental para que as Forças Armadas implementem medidas regulatórias adequadas para mitigar riscos e assegurar o desenvolvimento responsável (Gaire, 2023; Zhang et al., 2020), com atenção a armadilhas potenciais e que tarefas podem ser beneficiadas ou prejudicadas pela IA.

REFERÊNCIAS BIBLIOGRÁFICAS

Bitzinger, R. & Raska, M. (2022). *Chinese and Russian Military Modernization and the Fourth Industrial Revolution*. https://doi.org/10.1007/978-3-030-97012-3_7

Black, E. (2023). Consultants using AI do better, especially underperformers: study. [Online] Retirado de https://www.afr.com/work-and-careers/workplace/consultants-using-ai-do-better-especially-underperformers-study-20230922-p5e6vi#:~:text=Harvard%20Business%20School

Bokonda, P. L., Ouazzani-Touhami, K., & Souissi, N. (2020). *Predictive analysis using machine learning: Review of trends and methods*. https://doi.org/10.1109/isaect50560.2020.9523703

Candelon, F, Krayer, L., Rajendran, S. & Martinez, D. Z. (2023). *How People Can Create—and Destroy—Value with Generative AI*. [Online] Retirado de https://www.bcg.com/publications/2023/how-people-create-and-destroy-value-with-gen-ai

Dagnaw, G. A., Endeshaw, G. G. (2019). Current Trends of Artificial Intelligence in Nanosciences Application. *Nuclear Science, 4*(4), 60-65. https://doi.org/10.11648/j.ns.20190404.14

Davis P. K. & Bracken, P. (2022). Artificial intelligence for wargaming and modeling. *The Journal of Defense Modeling and Simulation*. https://doi.org/10.1177/15485129211073126

Jayakumar, P., Jhanjhi, N. Z., & Brohi, S. N. (2021). *Artificial Intelligence and Military Applications: Innovations, Cybersecurity Challenges & Open Research Areas*. https://doi.org/10.20944/preprints202108.0047.v1

Gaire, U. S. (2023). Application of Artificial Intelligence in the Military: An Overview. *Unity Journal, 4*(1), 161–174. https://doi.org/10.3126/unityj.v4i01.52237

Horowitz, M. C., Kahn, L. & Mahoney, C. (2020). The Future of Military Applications of Artificial Intelligence: A Role for Confidence-Building Measures?, *Orbis, 64*(4), 528-543. https://doi.org/10.1016/j.orbis.2020.08.003

Noy S., Zhang, W. (2023). Experimental evidence on the productivity effects of generative artificial intelligence. *Science, 381*(6654), 187-192. https://doi.org/10.1126/science.adh2586

Rashid, A. B., Kausik, A. K., Al Hassan Sunny, A., & Bappy, M. H. (2023). Artificial Intelligence in the Military: An Overview of the Capabilities, Applications, and Challenges, *International Journal of Intelligent Systems, 8676366,* https://doi.org/10.1155/2023/8676366

Rickli, J. & Mantellassi, F. (2023). *Peace of Mind: Cognitive Warfare and the Governance of 21st Century Subversion*.

Sadiku, M., Ashaolu, T. J., Ajayi-Majebi, A. & Musa, S. (2021). Artificial Intelligence in Social Media. *International Journal Of Scientific Advances. 2*. https://doi.org/10.51542/ijscia.v2i1.4

Steff, R. & Abbasi, K. (2020). Artificial intelligence and the military balance of power. https://doi.org/ 10.4324/9780367808846-6

Șușnea, E., & Buță, I. (2021). Artificial Intelligence in Hybrid Warfare: A Literature Review and Classification. Strategies Xxi - Security and Defense Faculty.

Zhang, Y., Zhang, L., Dai, Z., Chen, L., Zhou, Y., & Wang, Z. (2020). *Application of Artificial Intelligence in Military: From Projects View*. https://doi.org/10.1109/bigdia51454.2020.00026

ESTUDO 1 – INTELIGÊNCIA ARTIFICIAL: CONTRIBUTOS PARA UMA ESTRATÉGIA NA ÁREA DA DEFESA[1]

ARTIFICIAL INTELLIGENCE: CONTRIBUTIONS TO A DEFENSE STRATEGY

Jorge Manuel Nogueira Paiva
Capitão-de-mar-e-guerra

Armando José Dias Correia
Comodoro

RESUMO

A Organização do Tratado Atlântico Norte (OTAN) e as organizações de defesa dos Aliados estão a implementar estratégias para o desenvolvimento, adoção e utilização da Inteligência Artificial (IA). Na área da Defesa, em Portugal, ainda não há iniciativas estratégicas para o desenvolvimento, adoção e utilização da IA. Este estudo tem o objetivo de identificar um conjunto de contributos para a definição duma estratégia que permita colmatar esta lacuna. Para desenvolver esta investigação adotou-se uma metodologia assente num processo de raciocínio dedutivo, recorrendo a uma estratégia mista, baseada no estudo de caso. A investigação começa por identificar os aliados da OTAN que se constituem como referências no âmbito da IA, os princípios e um modelo orientador para o desenvolvimento, adoção e utilização da IA na área da Defesa. Seguidamente, analisou a IA na área da Defesa em Portugal, verificando-se que se encontra num patamar de maturidade inicial. No final, são apresentados contributos para uma estratégia de IA na área da Defesa, que procura um nível otimizado de desenvolvimento, adoção e utilização da IA e que deverá ser prosseguida através da criação duma estrutura de governação dedicada com monitorização e controlo da execução dos objetivos estratégicos.

Palavras-chave: Inteligência artificial, maturidade em inteligência artificial, gestão estratégica

[1] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Promoção a Oficial General (CPOG 2023-2024). A versão integral encontra-se disponível nos no Centro de Recursos do Conhecimento do Instituto Universitário Militar.

ABSTRACT

The North Atlantic Treaty Organisation (NATO) and Allied defence organisations are implementing strategies for the development, adoption and use of Artificial Intelligence (AI). In the area of Defence in Portugal, there are still no strategic initiatives for the development, adoption and use of AI. The aim of this study is to identify a set of contributions to the definition of a strategy to fill this gap. To carry out this research, a methodology based on a process of deductive reasoning was adopted, using a mixed strategy based on a case study.

The research begins by identifying the NATO allies that are references in the field of AI, the principles and a guiding model for the development, adoption and use of AI in the area of Defence. It then analysed AI in Defence in Portugal, finding that it is at an initial level of maturity. In the end, contributions are presented for an AI strategy in the area of Defence, which seeks an optimal level of development, adoption and use of AI and which should be pursued through the creation of a dedicated governance structure with monitoring and control of the implementation of strategic objectives.

***Keywords**: Artificial intelligence, artificial intelligence maturity, strategic management*

1. INTRODUÇÃO

> "This foundational technology will likely affect the full spectrum of activities undertaken by the Alliance in support of its three core tasks; collective defence, crisis management, and cooperative security."
> ((OTAN, 2021)

A Inteligência Artificial (IA), um campo das tecnologias emergentes e disruptivas (TED)[2], está na ordem do dia, sendo uma das áreas com maior potencial de desenvolvimento e na qual se depositam as maiores expetativas, canalizando um grande esforço de investimento (Tortoise, 2023).

No âmbito específico das organizações de defesa, o planeamento estratégico da IA está a revelar-se cada vez mais importante devido ao potencial transformador e disruptivo destas tecnologias nas guerras modernas e nas operações de segurança, tendo sido identificada a existência e o emprego operacional de várias aplicações militares da IA, podendo esta ser utilizada como facilitador analítico, disruptor de informação ou multiplicador de força (Raska & Bitzinger, 2023, p. 4).

[2] As TED referem-se a um conjunto de avanços tecnológicos em rápida evolução que têm um impacto significativo em vários aspetos da sociedade, incluindo a defesa e a segurança (OTAN, 2024).

Em setembro de 2017, Putin dirigiu-se a estudantes russos informando-os de que a IA é o futuro, não só da Rússia, mas de toda a humanidade. Disse também que quem se tornar o líder na esfera das tecnologias da IA governará o mundo e que por isso será melhor evitar que alguém consiga o monopólio das mesmas (Cable News Network, 2017).

Em 2017, a China publicou o seu plano estratégico *New Generation Artificial Intelligence Development Plan* assumindo o desígnio de se tornar o líder mundial desta área tecnológica até 2030. Esta estratégia reconhece que, ao fim de cerca de 60 anos de evolução, a IA entrou numa nova fase, tornou-se num novo foco de competição internacional, concentrando a atenção dos países mais desenvolvidos do mundo por considerarem o desenvolvimento da IA como uma das principais estratégias para melhorar a sua competitividade e proteger eficazmente a sua segurança nacional (DigiChina, 2017).

A Ordem Executiva n.º 13859 (2019, p. 3967) estabelece que *"Continued American leadership in AI is of paramount importance to maintaining the economic and national security of the United States and to shaping the global evolution of AI in a manner consistent with our Nation's values, policies, and priorities"*. O documento estratégico *National Artificial Intelligence Research And Development Strategic Plan: 2023 Update* mantém o desígnio dos Estados Unidos de conservarem a liderança no desenvolvimento e utilização de sistemas de IA (Select Commitee On Artificial Intelligence, 2023, p. vii).

Segundo a Organização para a Cooperação e o Desenvolvimento Económicos (OCDE, 2023), muitos foram os países que, desde 2017, publicaram as suas iniciativas estratégicas nacionais de IA. Portugal não constitui exceção nesta matéria, tendo publicado a sua estratégia nacional para a IA em 2019 (Portugal INCoDe.2030, 2019).

A Organização do Tratado do Atlântico Norte (OTAN) definiu a sua estratégia para a IA em 21 de outubro de 2021. Esta estratégia identifica como a IA pode ser aplicada à defesa e segurança de forma ética e protegida, estabelecendo padrões de utilização responsável das tecnologias de IA de acordo com o direito internacional e os valores da OTAN. Aborda ainda as ameaças colocadas pela utilização da IA por adversários e como estabelecer uma cooperação baseada na confiança com a comunidade de inovação em IA (OTAN, 2021).

Os Estados Unidos da América (EUA) e a França são exemplos de aliados que referem o desenvolvimento da IA no âmbito militar nos seus planos estratégicos nacionais e, adicionalmente, desenvolveram planos estratégicos específicos para

a aplicação militar da IA, no âmbito das suas organizações de defesa. Contudo, verifica-se que muitos planos estratégicos nacionais não referem expressamente objetivos ou linhas de ação estratégicas relativas à aplicação da IA no setor da Defesa (OCDE, 2021, p. 10).

De acordo com o *Cooperative Cyber Defence Centre of Excellence* da OTAN (CCDCOE, 2021, p. 24), nem todos os países da OTAN desenvolveram planos estratégicos específicos para as aplicações militares da IA. É o caso de Portugal que, apesar de ter uma estratégia nacional para a IA, não faz qualquer referência ao seu desenvolvimento no âmbito da Defesa (Portugal INCoDe.2030, 2019).

A presente investigação tem, assim, por objeto o desenvolvimento, adoção e utilização da IA na área da Defesa , tutelada pelo Ministério da Defesa Nacional (MDN). O propósito deste estudo é propor contributos para uma estratégia de IA na área da Defesa.

O Objetivo Geral (OG) do presente estudo é "Propor contributos para uma estratégia de inteligência artificial na área da Defesa", integrando os seguintes Objetivos Específicos (OE): analisar a IA no ambiente externo à área da Defesa; analisar a IA na área da Defesa.

Estruturalmente, o trabalho foi desenvolvido em cinco capítulos. O primeiro corresponde à presente introdução. O segundo, apresenta o enquadramento teórico e conceptual da investigação. O terceiro e quarto analisam e caracterizam o ambiente externo e o ambiente interno da área da Defesa, respetivamente. O quinto apresenta os contributos para uma estratégia de IA na área da Defesa. Finalmente, o sexto e último, apresenta as conclusões, contributos para o conhecimento, limitações, estudos futuros e recomendações.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

Neste capítulo apresenta-se a revisão da literatura relativa aos três conceitos estruturantes (inteligência artificial, maturidade em inteligência artificial e gestão estratégica) e o modelo de análise.

2.1. Inteligência Artificial

A criação do termo do termo "Inteligência Artificial" é atribuída a John McCarthy, um investigador do *Massachusetts Institute of Technology* e pioneiro nos campos da IA, ciência dos computadores e sistemas de computação interativos (Springer, 2023).

John McCarthy (2007, p. 2) definiu IA como "*It is the science and engineering of making intelligent machines, especially intelligent computer programs*".

Deste modo, a IA não é uma tecnologia ou método técnico específico, mas sim um ramo da área das ciências da computação, que procura conseguir desenvolver inteligência produzida por máquinas (OTAN, 2005). Não obstante o acima referido, não existe uma definição universal e consensual de IA, apresentando-se seguidamente algumas definições relevantes:

- A OTAN definiu IA como "*The branch of computer science devoted to developing data processing systems that perform functions normally associated with human intelligence, such as reasoning, learning, and self-improvement*" (OTAN, 2005).

- Em 2020, o *National Artificial Intelligence Initiative Act of 2020* dos EUA definiu IA como "*a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments*" (House of Representatives, 2020, p. 5).

- O n.º 1 do artigo 3.º do Artificial Intelligence Act, da União Europeia (UE) define IA como:

> […] *a machine-based system designed to operate with varying levels of autonomy, that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments*. (Parlamento Europeu, 2024)

Face às diversas definições elencadas, dada a multidisciplinaridade requerida para o seu desenvolvimento e a transversalidade das suas potenciais aplicações, bem como dependendo duma abordagem mais técnica ou mais filosófica, pode-se concluir que não existe atualmente uma definição consensual do que é IA. As definições supracitadas encaram a IA como uma área científica e/ou tecnológica que cria sistemas de IA, ou alternativamente consideram os próprios sistemas como o ponto de partida da definição de IA, ou seja, nesta perspetiva a IA não é uma disciplina científica ou área tecnológica, mas os sistemas por elas criados.

Não obstante o acima referido, da comparação das diversas definições, a IA surge como uma área científica e/ou tecnológica, que desenvolve sistemas que utilizam programas e equipamentos físicos para executar, com diversos graus de autonomia, tarefas normalmente associadas à inteligência humana.

Neste sentido, considera-se que a definição de IA estabelecida pela iniciativa estratégica portuguesa (Portugal INCoDe.2030, 2019, p. 16) como a "área científica e o conjunto de tecnologias que utilizam programas e dispositivos físicos para imitar facetas avançadas da inteligência humana" reúne os elementos principais das definições acima elencadas e, por motivo de coerência do edifício estratégico nacional, assume-se como referência para o conceito de IA no âmbito deste estudo.

2.2. Maturidade em Inteligência Artificial

A elaboração duma estratégia inicia-se com a definição de um ponto de partida, o que no âmbito da IA requer um diagnóstico da maturidade da organização em IA. Os modelos de maturidade (MM) têm uma longa história e existem muitos modelos na literatura dirigidos a determinados tópicos, oferecendo às organizações uma forma simples e eficaz de medir as suas capacidades numa determinada área (Leino et al., 2017, p. 37).

Os Modelos de Maturidade (MM) também têm desempenhado um papel crucial na avaliação da prontidão organizacional para tirar partido da IA. Os MM da IA (MMIA) são ferramentas fundamentais para avaliar e melhorar as capacidades organizacionais relacionadas à IA, orientando ações e comparações. Estes modelos permitem avaliar a capacidade de utilização da IA, orientando a progressão rumo aos objetivos de IA desejados. A literatura e informação pública disponível oferecem uma ampla gama de trabalhos e ferramentas para avaliar a Maturidade em IA (MIA) nas organizações, identificando as dimensões-chave e avaliando essas capacidades em níveis de maturidade, permitindo conhecer o estado da adoção das tecnologias de IA em cada área (Sadiq et al., 2021).

Desta forma, a MIA duma organização não é mais que o estado de adoção interna da IA, que pode ser aferido através da aplicação de um MMIA que afere níveis de maturidade, permitindo verificar o nível de maturidade em que a organização se encontra, estabelecer qual o nível de maturidade que a liderança quer atingir e definir as consequentes linhas de ação para atingir o nível de maturidade superior.

Para a avaliação do estado atual da MIA na área da Defesa, decorrente da análise efetuada de dez MMIA, optou-se pela o modelo da MITRE *Corporation* (MITRE Corporation, 2023). Esta escolha justifica-se por ser um modelo muito recente que contempla as várias dimensões de interesse face às últimas abordagens organizacionais de IA (designadamente da OTAN, UE e EUA). Realça-se que este modelo avalia aspetos como a responsabilidade, transparência e confiança dos

utilizadores, sendo o único modelo encontrado que disponibiliza publicamente os instrumentos de diagnóstico para avaliação do nível de MIA.

Este modelo, que se encontra melhor detalhado no Apêndice A, foi desenvolvido com base numa análise sistemática dos MMIA comerciais existentes no sector privado, bem como na apreciação dos processos de avaliação da Integração do Modelo de Maturidade das Capacidades desenvolvidos pela *Universidade Carnegie Mellon* e das Normas de IA do Instituto Nacional de Normas e Tecnologia dos EUA, ou seja, tem uma base empírica, científica e normativa (MITRE Corporation, 2023, p. III).

Através da Figura 1, pode-se observar que o modelo comporta 20 dimensões que se distribuem por 6 pilares e permite classificar a organização em 5 níveis de maturidade, desde o "Nivel 1 – Inicial" até ao "Nível 5 – Otimizado".

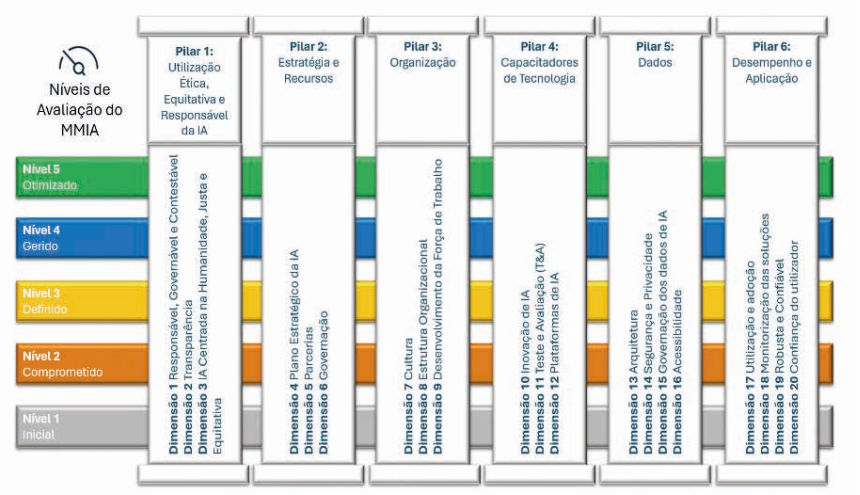

Figura 1 – Visão geral do MMIA: Pilares, dimensões e níveis de avaliação
Fonte: Adaptado de Mitre Corporation (2023, p. 3).

2.3. Gestão Estratégica

O processo estratégico inicia-se com a caracterização da situação da organização comparativamente com os seus concorrentes, identificando oportunidades e ameaças, sejam internas ou externas. No Estado-Maior-General das Forças Armadas (EMGFA) e na Marinha (Figura 2) o modelo compreende

sete etapas que ocorrem de forma sequencial, cíclica e que se agrupam em três fases (formulação, operacionalização e controlo) com a função de promover a transformação contínua da organização (Ribeiro & Pinto, 2022, pp. 28-30).

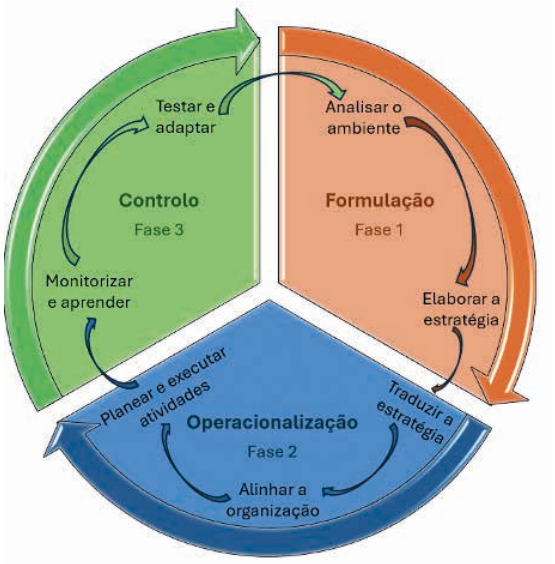

Figura 2 – Modelo do processo estratégico
Fonte: Adaptado a partir de Ribeiro e Pinto (2022, p. 30).

As fases da gestão estratégica permitem classificar a situação da implementação de uma estratégia e possibilitam a apresentação de contributos de uma forma estruturada.

Por seu turno, o mapa estratégico permite apresentar os objetivos estratégicos organizados em três perspetivas de gestão, complementares e interdependentes: genética, estrutural e operacional, que contribuem para uma perspetiva de topo, relativa à missão (Ribeiro & Pinto, 2022). Segundo estes autores as adaptações são válidas, desde que se consiga uma descrição adequada da estratégia organizacional, isto é, que seja possível fundamentar a relação de causa-efeito entre as referidas perspetivas de gestão e os respetivos objetivos estratégicos (Ribeiro & Pinto, 2022, p. 71).

As linhas de ação são validadas recorrendo às provas da estratégia: adequabilidade, exequibilidade e aceitabilidade (Ribeiro, 2009, pp. 190-195).

2.4. Modelo de análise

No Quadro 1 apresenta-se o modelo de análise utilizado nesta investigação.

Quadro 1 – Modelo de análise

<table>
<tr><td>Objetivo Geral (OG)</td><td colspan="5">Propor contributos para uma estratégia de inteligência artificial na área da Defesa.</td></tr>
<tr><td>Questão Central (QC)</td><td colspan="5">Que contributos se podem alinhar para o desenvolvimento de uma estratégia de inteligência artificial na área da Defesa?</td></tr>
<tr><td>Objetivos Específicos (OE)</td><td>Questões Derivadas (QD)</td><td>Conceitos Estruturantes</td><td>Dimensões</td><td>Indicadores</td><td>Técnicas de recolha de dados</td></tr>
<tr><td rowspan="2">OE1
Analisar a IA no ambiente externo à área da Defesa.</td><td rowspan="2">QD1
Como se caracteriza a abordagem estratégica da IA na OTAN e organizações de defesa dos países-membros de referência?</td><td rowspan="2">Inteligência Artificial (IA)</td><td rowspan="5">Vinte dimensões, agrupadas em seis pilares (ver Apêndice C):
Utilização Ética, Equitativa e Responsável da IA
Estratégia e Recursos
Organização
Capacitadores de Tecnologia
Dados
Desempenho e Aplicação</td><td>Impulsionadores
Obstáculos
Princípios
Oportunidades
Ameaças</td><td>Análise documental</td></tr>
<tr><td rowspan="3">OE2
Analisar a IA na área da Defesa.</td><td rowspan="3">QD2
Como se caracteriza a abordagem estratégica da IA na área da Defesa?</td><td rowspan="2">Maturidade em Inteligência Artificial (MIA)</td><td>Potencialidades
Vulnerabilidades
Nível de MIA</td><td>Análise documental
Questionário de MIA</td></tr>
<tr><td>Gestão Estratégica</td><td>Provas da Estratégia</td><td>Entrevistas de validação</td></tr>
</table>

No presente estudo foram utilizados um raciocínio dedutivo, uma estratégia mista (qualitativa e quantitativa) e um desenho de pesquisa do tipo estudo de caso (Santos & Lima, 2019, pp. 22-37). Os dados qualitativos ordinais suportaram um diagnóstico de MIA, que contribuiu para a análise do ambiente interno.

Os dados recolhidos permitiram o desenvolvimento dum processo estratégico (Ribeiro & Pinto, 2022) atinente à apresentação de contributos para uma estratégia de IA na área da Defesa.

Participantes: Integraram esta investigação dezanove organismos da área da Defesa:

– As Forças Armadas (FA) – EMGFA, Marinha, Exército e Força Aérea;

– Autoridades – Autoridade Aeronáutica Nacional (AAN) e Autoridade Marítima Nacional (AMN).

– Os Serviços Centrais – Secretaria-Geral do Ministério da Defesa Nacional (SGMDN), Inspeção-Geral da Defesa Nacional (IGDN), Direção-Geral da Política da Defesa Nacional (DGPDN), Direção-Geral de Recursos da Defesa Nacional (DGRDN), Instituto da Defesa Nacional (IDN) e Polícia Judiciária Militar (PJM);

– A idD – Portugal Defence (idD) e empresas participadas – Arsenal do Alfeite, S.A. (AA); ETI – Empordef Tecnologias de Informação, S.A. (ETI); NavalRocha

– Sociedade de Construção e Reparações Navais, S.A. (NavalRocha); OGMA – Indústria Aeronáutica de Portugal, S.A. (OGMA); EID – Empresa de Investigação e Desenvolvimento de Eletrónica, S.A. (EID) e Thales Edisoft Portugal, S.A. (Edisoft).

Para efeitos de validação, o presente estudo foi enviado a 11 especialistas com conhecimento relevante do objeto desta investigação.

Procedimento. Tendo sido necessário traduzir um questionário existente, o mesmo foi remetido para análise e validação a um grupo de peritos da área das tecnologias de informação (Hill & Hill, 2008, pp. 77-82). Depois de integrados os *feedbacks* entretanto recebidos, o questionário foi enviado, em fevereiro de 2024, para as entidades acima identificadas, e as respostas recolhidas no período de 15 de fevereiro a 15 de março de 2024.

Para avaliação da MIA na área da Defesa, foi aplicado um questionário com 20 questões fechadas e uma questão aberta sobre IA. O questionário foi aplicado a 19 organismos da área da Defesa que se considerou como a população-alvo. Cada organismo preencheu apenas um questionário. Obtiveram-se 16 respostas não probabilísticas voluntárias refletindo o posicionamento de cada organismo relativamente às questões colocadas. O IDN, a ETI e a NavalRocha não responderam.

Para recolha de contributos finais e validação do estudo, o mesmo foi distribuído em formato de *draft* final para aplicação das provas da estratégia aos contributos identificados.

Os níveis de maturidade, correspondendo a categorias ordenadas definidas arbitrariamente, constituem dados qualitativos e ordinais, apesar de serem expressos por números. Assim, recorrendo ao *Microsoft Excel*, foi realizada a análise estatística descritiva das respostas ao questionário.

Quanto às técnicas de tratamento e análise dos restantes dados qualitativos foi utilizada a análise de conteúdo proposta por Guerra (2006, cit. por Santos & Lima, 2019) designadamente através da transcrição (quando aplicável), leitura, construção de sinopses, análise descritiva e análise interpretativa.

3. A INTELIGÊNCIA ARTIFICIAL NO AMBIENTE EXTERNO À ÁREA DA DEFESA

Neste capítulo, utilizando um processo dedutivo, efetuou-se uma análise do ambiente externo, face às dimensões identificadas no modelo de análise, permitindo responder à QD1.

3.1. A Organização do Tratado do Atlântico Norte

Há mais de 70 anos que a OTAN se mantém na vanguarda tecnológica para assegurar a defesa dos seus países membros e o sucesso das suas operações. Em fevereiro de 2021, os Ministros da Defesa da OTAN endossaram "*Foster and Protect: NATO's Coherent Implementation Strategy on Emerging and Disruptive Technologies*", uma estratégia sobre TED para orientar o desenvolvimento da política da OTAN em áreas temáticas específicas (OTAN, 2023).

No âmbito das TED, as prioridades da OTAN incluem a IA, autonomia, computação quântica, biotecnologias e aperfeiçoamento humano, sistemas hipersónicos, espaço, novos materiais e processos de fabrico, energia e propulsão e redes de comunicações da próxima geração (OTAN, 2023).

O Conceito Estratégico da OTAN 2022 tem três pontos dedicados às TED reconhecendo que estas são simultaneamente oportunidades e ameaças e que estão a alterar o caráter dos conflitos, apresentando uma crescente relevância estratégica (OTAN, 2022).

No período de 20 a 22 de outubro de 2021, em Bruxelas, decorreu um encontro dos ministros da defesa da OTAN onde foi aprovada a sua estratégia para a IA, a qual reconhece que a IA está a alterar o ambiente global de defesa e segurança, constituindo-se como uma oportunidade para fortalecer a vantagem tecnológica da OTAN, mas simultaneamente também aumentará a velocidade das ameaças que a mesma terá de enfrentar (OTAN, 2021).

3.2. Os *Digital Leaders* da Organização do Tratado do Atlântico Norte

De forma a determinar quais são os países da OTAN, que devem ser tomados como referência no âmbito do desenvolvimento, adoção e utilização da IA, construiu-se um quadro comparativo (Quadro 2) que teve como ponto de partida o relatório do NATO *Cooperative Cyber Defence Centre of Excellence* (CCDCOE, 2021), identificando-se a situação de todos os países da OTAN. Do quadro realça-se a identificação dos *Digital Leaders* da Aliança[3].

[3] *Digital Leaders* - sistematização da situação dos aliados em termos de Tranformação Digital (TD). A análise pretendeu identificar os aliados mais avançados neste domínio (Correia, A. J. D., 2023).

Quadro 2 – Estratégia de IA na UE e OTAN

Países Membros da OTAN	UE	Digital Leaders	Estratégia Nacional para a IA	Estratégia do Organismo de Defesa para a IA
ALBÂNIA (2009)	N		N	N
ALEMANHA (1955)	S		S	N
BÉLGICA (1949)	S		S	N
BULGÁRIA (2004)	S		S	N
CANADÁ (1949)	N	S	S	S
CHÉQUIA (1999)	S		S	N
CROÁCIA (2009)	S		N	N
DINAMARCA (1949)	S		S	N
ESLOVÁQUIA (2004)	S		N	N
ESLOVÉNIA (2004)	S		S	N
ESPANHA (1982)	S	S	S	S
ESTADOS UNIDOS (1949)	N	S	S	S
ESTÓNIA (2004)	S		S	N
FINLÂNDIA (2023)	S	S	S	S
FRANÇA (1949)	S	S	S	S
GRÉCIA (1952)	S		N	N
HOLANDA (1949)	S		S	N
HUNGRIA (1999)	S		S	N
ISLÂNDIA (1949)	N		S	N
ITÁLIA (1949)	S		S	N
LETÓNIA (2004)	S		S	N
LITUÂNIA (2004)	S		S	N
LUXEMBURGO (1949)	S		S	N
MACEDÓNIA DO NORTE (2	N		N	N
MONTENEGRO (2017)	N		N	N
NORUEGA (1949)	N	S	S	S
POLÓNIA (1999)	S		S	N
PORTUGAL (1949)	S		S	N
REINO UNIDO (1949)	N	S	S	S
ROMÉNIA (2004)	S		S	N
TURQUIA (1952)	N		S	N

Fonte: adaptado de (CCDCOE, 2021, p. 24).

Através do Tabela 1 pode-se observar que todas as organizações de defesa dos sete *Digital Leaders* da OTAN já publicaram as respetivas estratégias de IA.

Tabela 1 – Os documentos da estratégia de IA na área da Defesa dos *Digital Leaders*

Aliado	Principais documentos disponíveis *online*
Canadá	*The Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy* (Department of Nacional Defence and Canadian Armed Forces, 2024)
França	*Artificial Intelligence in Support of Defence* (Ministére des Armées, 2019)
Noruega	*Strategi for kunstig intelligens for forsvarssektoren* (Forsvarsdepartementet, 2023)
Espanha	*Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en el Ministerio de Defensa* (Resolución 11197/2023, de 29 de junio, de la Secretaria de Estado de Defensa, 2023)

[Cont.]

EUA	*Department of Defense AI Strategy* (Department of Defense, 2018) *Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway* (Department of Defense, 2022) *Department of Defense Data, Analytics, and Artificial Intelligence Adoption Strategy* (Department of Defense, 2023)
Finlândia	*Strategic guidelines for DEVELOPING AI SOLUTIONS* (Finnish Ministry of Defence, 2020)
Reino Unido	*Defence Artificial Intelligence Strategy* (Ministry of Defence, 2022)

Da análise da documentação identificada na referida tabela resulta que todos os *Digital Leaders* criaram ou tencionam criar estruturas organizacionais destinadas à liderança e governação do desenvolvimento, adoção e utilização da IA na área da Defesa, podendo também incluir a implementação das estratégias de TD e Dados. Essas estruturas organizacionais encontram-se inseridas nas respetivas organizações de defesa, na dependência do Secretário de Estado da Defesa (EUA, Reino Unido e Noruega), da Direção Geral do Armamento (França e Espanha) ou do Chefe das Forças de Defesa (Finlândia).

3.3. Impulsionadores e obstáculos ao desenvolvimento, adoção e utilização da inteligência artificial na área da Defesa

Através da análise documental das estratégias de IA dos aliados *Digital Leaders* foi possível determinar os principais impulsionadores (Tabela 2) e obstáculos (Tabela 3) identificando-se a negrito as dimensões do MMIA mais relevantes.

Tabela 2 – Impulsionadores do desenvolvimento, adoção e utilização da IA

Fatores chave
Assegurar a vantagem estratégica, operacional e tecnológica, face à alteração do carácter do conflito num ambiente de competição global caracterizado por um clima de incerteza e instabilidade internacionais, atores estatais e não estatais, ameaças acima e abaixo do limiar da guerra e desenvolvimento e evolução do conceito de operações multidomínio, que incluem o espaço e o ciberespaço.
Maximizar a eficiência da organização, desde as funções administrativas até às operações no campo de batalha.
Garantir o alinhamento e integração, com as estratégias e soluções de IA da OTAN e países aliados, de modo a manter a interoperabilidade e a relevância das nossas forças.

[Cont.]

Assegurar métodos eficientes e eficazes, para o tratamento tempestivo do manancial de dados cuja quantidade tem assistido a um crescimento exponencial.
Contribuir para uma utilização Ética, Responsável, Legal e Transparente da IA.
Garantir o alinhamento com as estratégias e políticas nacionais para a IA
Aumento da capacidade e proteção do pessoal, através de uma abordagem Humano-Máquina concretizando o "efeito multiplicador" resultante da combinação da cognição e da inventividade humanas com as capacidades analíticas da velocidade das máquinas. A integração da IA nos sistemas utilizados pelas FA também reduz os riscos de morte e lesão do pessoal.
Preservar a resiliência e a capacidade de atualização dos sistemas, a robustez e a resiliência são questões críticas num ambiente em que o sucesso dos compromissos depende das redes de comunicação e do acesso à informação.
Beneficiar da utilização dual e específica das tecnologias de IA, quer através da utilização direta de soluções civis (por exemplo: logística, apoio ao ciclo de vida e gestão de pessoal), quer adaptando ou desenvolvendo soluções para outras necessidades do setor de defesa.

Tabela 3 – Obstáculos ao desenvolvimento, adoção e utilização da IA nos Aliados

Obstáculos à mudança (âmbito e descrição sumária)
Estratégia: A ausência de orientações estratégicas para a IA, prejudica e pode impedir o alinhamento e articulação das ações, a obtenção dos resultados esperados, o cumprimento dos objetivos definidos.
Liderança: A falta de conhecimento basilar e estratégico da IA e das suas implicações, pelos líderes da organização, dificulta e pode impedir a implementação da IA na organização.
Governação: A inexistência ou deficiência de órgãos de governação, de um enquadramento normativo e de um ambiente de controlo, dificulta e pode impedir a implementação da IA.
Organização: A organização deve adaptar-se para a IA, desenvolvendo uma estrutura organizacional adequada à IA (cargos, respetivas competências e responsáveis) pois caso contrário pode inviabilizar a implementação da IA.
Talento: A falta de competências no âmbito da IA constitui um sério obstáculo ao desenvolvimento, adoção e utilização da IA.
Dados: Existem dificuldades em garantir a disponibilidade de dados de alta qualidade, seguros, estruturados, exploráveis e acessíveis para aplicações de IA.
Plataformas/Infraestruturas tecnológicas: A desatualização, obsolescência, desarticulação e insegurança das plataformas tecnológicas prejudicam o desenvolvimento e utilização da IA.
Requisitos militares complexos e em evolução: A tecnologia em geral e a IA em particular evoluem a um ritmo exponencial dificultando o planeamento de capacidades e a adaptação da indústria de defesa.
Financiamento para o desenvolvimento tecnológico: O financiamento público, tanto nacional como internacional, é crucial para o desenvolvimento das capacidades de IA.
Riscos e vulnerabilidades tecnológicas: As tecnologias de IA, especialmente no início, apresentam vários riscos, como a manipulação, o enviesamento e resultados opacos. Assumem particular importância a cibersegurança e segurança da informação nas Tecnologias de Informação.
Afetação de recursos: A necessidade de um investimento substancial em recursos humanos e tecnológicos para apoiar a adoção da IA pode constituir um obstáculo significativo.

[Cont.]

Mudança cultural: Vencer a resistência à mudança e transformar a cultura organizacional existente numa cultura ágil, integrada e preparada para tirar partido das tecnologias de IA exige um esforço substancial e uma gestão da mudança.

3.4. Princípios orientadores para o desenvolvimento, adoção e utilização da inteligência artificial na área da Defesa

Em resultado da análise documental das iniciativas estratégicas para o desenvolvimento, adoção e utilização da IA em curso nos *Digital Leaders* da OTAN, sintetizaram-se as principais soluções por eles identificadas. A Tabela 4 sistematiza os princípios a observar no desenvolvimento, adoção e utilização da IA, com base nas soluções apontadas pelos aliados *Digital Leaders*, assinalando-se a negrito e sublinhado as dimensões mais relevantes.

Tabela 4 – Princípios do desenvolvimento, adoção e utilização da IA na área da Defesa

Princípios
Garantir o cumprimento dos princípios da utilização responsável da IA, designadamente: Legalidade; Ética; Responsabilidade e Prestação de Contas; Explicabilidade e Rastreabilidade; Transparência; Fiabilidade; Governação; Mitigação do Enviesamento/Preconceito; Segurança e; Privacidade.
Estabelecer a liderança e a governação do processo de implementação da estratégia de IA, designadamente através da nomeação de responsáveis, da criação duma estrutura central e transversal para o efeito e de mecanismos de controlo da execução da estratégia.
Alocar financiamento aos investimentos em IA e Tecnologia, através da afetação do orçamento da Defesa e explorando programas/mecanismos de financiamento nacionais e internacionais.
Fomentar as parcerias intergovernamentais, académicas, industriais e com outras agências, nacionais e internacionais, para permitir o rápido desenvolvimento, adoção e utilização de IA. Esta interação deve contribuir para estimular a inovação e a investigação em domínios específicos e captar desenvolvimentos que possam ser implementados nos sistemas utilizados pelas FA, pelas administrações e pelos serviços de apoio.
Garantir a cooperação, alinhamento e integração com as estratégias, Planos, Programas e soluções de IA da OTAN e países aliados, reforçando a comunicação e interoperabilidade de dados, software e sistemas.
Promover a mudança cultural, através da adoção duma cultura de inovação, proativa, adaptativa, colaborativa, transversal, de segurança, orientada para os dados e "*agile*". Adicionalmente, deve ser fomentada a literacia em IA, TD e Dados.
Edificar e gerir a Força de Trabalho de IA, através de: definição de uma carreira de IA e de um chefe de classe profissional; criação de cargos e definição das respetivas competências; identificar e empregar o talento existente e; assegurar o recrutamento, formação e retenção do talento necessário ao desenvolvimento, adoção e utilização da IA.

[Cont.]

Fomentar o intercâmbio e parcerias de lideranças e talentos entre a Defesa, o meio académico e o sector tecnológico: estabelecendo mecanismos de colocação expeditos para líderes civis talentosos no domínio da IA; desenvolvendo iniciativas para os líderes da Defesa adquirirem experiência no setor tecnológico; potenciando as intervenções apoiadas pelo governo ao nível dos melhores talentos, dos doutoramentos e dos mestrados; Fomentando protocolos para a colocação de estudantes de mestrado em IA na área da Defesa, de forma a adquirirem experiência prática na Defesa e; promovendo programas nacionais de competências para aumentar o volume de talentos em áreas críticas.
Promover a Inovação em IA, assegurando o rápido desenvolvimento e fornecimento de capacidades através duma abordagem *"agile"*.
Adotar uma abordagem Humano-Máquina, maximizando o "efeito multiplicador" que advém da combinação da cognição e da inventividade humanas com as capacidades analíticas da velocidade das máquinas.
Assegurar a capacidade de teste e certificação, de forma a assegurar que as novas capacidades de IA são seguras, robustas, eficazes e ciberseguras.
Disponibilizar infraestruturas/plataformas tecnológicas resilientes, interoperáveis e transversais à área da Defesa, modernizar as infraestruturas de C5ISR e proteger as redes, aplicações, ativos e serviços através duma abordagem de cibersegurança *"Zero Trust"*.
Edificar o "Digital Backbone" da Defesa, um "ecossistema" que combina pessoas, processos, dados e tecnologia.
Reconhecer os Dados como recurso estratégico, definindo e implementando uma Estratégia de Dados, para garantir o acesso seguro a dados de alta qualidade, bem governados, com uma arquitetura adequada e devidamente classificados, o que assenta no controlo do ciclo de vida dos dados, desde a geração até à valorização, incluindo a produção, o processamento e o armazenamento (*"Big Data"*).
Explorar a natureza de Duplo Uso da IA, apoiando-se num ecossistema de dupla utilização, e aceder a capacidades de IA de interesse para a área da Defesa através da aquisição de software e suporte para estas soluções comerciais, libertando o talento da Defesa para desafios inerentemente militares.
Monitorização das soluções de IA, através da instrumentação e novas formas de recolher dados relevantes para a IA, exigindo que os produtos e serviços de software tenham a capacidade de disponibilizar dados de utilização e de desempenho.
Assegurar a confiança do utilizador, assegurando que: os utilizadores têm a formação, a compreensão e a experiência adequadas; mecanismos de ética, garantia e conformidade reconhecidos e; a verificação, validação e certificação permanentemente das capacidades de IA.

3.5. A União Europeia

A UE apresentou a sua estratégia de IA a 25 de abril de 2018, a qual reconhece as oportunidades e ameaças que a IA representa. Esta estratégia identifica os valores e pontos fortes da UE que devem ser capitalizados, definindo os seguintes objetivos: reforçar a capacidade industrial e tecnológica da UE e a adoção da IA na economia; preparar a UE para as mudanças socioeconómicas decorrentes da IA; garantir um quadro ético e jurídico apropriado (Comissão Europeia, 2018).

Em 2024, o Concelho Europeu aprovou o projeto final do *AI Act* proposto pela Comissão Europeia em 2021. Este marco histórico representa o primeiro

enquadramento legal global sobre IA, abordando riscos e consolidando a liderança europeia em regulação. Junto com o Pacote de Inovação da IA e o Plano Coordenado para a IA, o *AI Act* forma um conjunto abrangente de políticas para promover uma IA confiável. Essas medidas visam garantir segurança e direitos fundamentais, impulsionar a adoção, investimento e inovação em IA em toda a União Europeia (Comissão Europeia, 2024).

3.6 A Administração Pública

Como já foi referido, acompanhando o ímpeto internacional no âmbito da publicação das iniciativas estratégicas nacionais de IA, Portugal publicou a sua estratégia nacional para a IA em 2019 (Portugal INCoDe.2030, 2019).

Esta estratégia pretende a promoção e a mobilização da sociedade em geral para o ensino e investigação, para a inovação e desenvolvimento de produtos e serviços suportados em tecnologias IA e encontra-se alinhada com o Plano de Ação da UE e dos seus estados-membros, o qual promove o uso da IA na resolução de desafios globais, como a saúde, clima, agricultura ou a cibersegurança (Portugal INCoDe.2030, 2019, p. 9). Releva-se que a iniciativa estratégica em apreço não faz qualquer alusão à sua potencial aplicação no âmbito da Defesa Nacional.

Adicionalmente, a nível nacional foram promovidas várias iniciativas estratégicas que potenciam o desenvolvimento, adoção e utilização da IA (Tabela 5).

Tabela 5 – Estratégias nacionais relacionadas com a IA

#	Estratégia	Versão	Fonte
1	Estratégia Nacional de Segurança do Ciberespaço	2019	(Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho)
2	Plano de Ação para a Transição Digital	2020	(Resolução do Conselho de Ministros n.º 30/2020, de 21 de abril)
3	Estratégia *Cloud* para a Administração Pública em Portugal	2020	(Conselho para as Tecnologias de Informação e Comunicação na Administração Pública, 2020)
4	Estratégia para a TD da Administração Pública 2021-2026 e respetivo Plano de Ação Transversal para o período 2021-2023.	2021	(Resolução do Conselho de Ministros n.º 131/2021, de 10 de setembro)
5	Plano de Recuperação e Resiliência (PRR) - Digital		(Recuperar Portugal, s.d.)
6	Estratégia Nacional de Dados	2022	(Portugal Digital, 2022)
7	Estratégia Nacional de Inteligência Artificial	2022	(Portugal INCoDe.2030, 2019)
9	Estratégia Nacional de Computação Avançada	2023	(Fundação para a Ciência e Tecnologia, 2023)

3.7. Síntese conclusiva e resposta à Questão Derivada 1

A OTAN aprovou a sua estratégia para a IA em fevereiro de 2021 estabelecendo quatro objetivos estratégicos onde se destacam os princípios da utilização responsável da IA. Os sete *Digital Leaders* da OTAN publicaram estratégias específicas e autónomas para o desenvolvimento, adoção e utilização da IA.

Através da análise da documentação estratégica relativa à IA da OTAN e dos seus *Digital Leaders*, foram identificados os principais impulsionadores, obstáculos e princípios do desenvolvimento, adoção e utilização da IA nas organizações de Defesa. Um dos objetivos da estratégia de IA da UE, consiste em garantir um quadro ético e jurídico apropriado, designadamente através do *AI Act*. Em Portugal, a Administração Pública definiu estratégias para a IA, transição digital, dados, computação avançada, *Cloud*, e segurança do ciberespaço.

Neste contexto, as potenciais oportunidades e ameaças que poderão afetar a IA na área da Defesa encontram-se identificadas nas Tabelas 1 e 2, respetivamente.

Tabela 6 – Oportunidades

	Oportunidades	Fonte
O1	A integração da IA permite melhorar a eficiência das organizações	*Digital Leaders*
O2	Assegurar a vantagem tecnológica e decisória no âmbito das operações multidomínio, no respeito pelos princípios da Utilização Ética, Equitativa e Responsável da IA	*Digital Leaders*
O3	Colaboração e participação em projetos nacionais e internacionais (OTAN, UE e AP)	OTAN, UE e AP
O4	Envolvimento da indústria, centros de investigação e universidades no fortalecimento das capacidades militares	*Digital Leaders*, OTAN, UE e AP
O5	Membros da OTAN mais avançados em IA, Dados e TD podem servir de modelo	*Digital Leaders*
O6	Sistemas, sensores e armas geram cada vez mais dados úteis à decisão	*Digital Leaders*
O7	Empenho da OTAN, UE e AP no desenvolvimento da IA e inovação (estratégias, programas, apoios à economia, I&D e indústria de Defesa	OTAN, UE, AP
	Ameaças	**Fonte**
A1	Maior capacidade de interferência na sociedade por atores externos (estatais e não estatais)	*Digital Leaders*
A2	Aumento da concorrência global, caracterizada por novas ameaças híbridas multidomínio com capacidades digitais, acima e abaixo do limiar do conflito armado	*Digital Leaders*
A3	O potencial excesso de dependência da IA, poderá levar à perda de perícias/competências humanas, o que pode dificultar o cumprimento das missões quando a utilização da IA é negada.	Digital Leaders

[Cont.]

A4	Risco da irrelevância junto dos Aliados, se não se acompanhar as iniciativas de IA dos Digital Leaders da OTAN.	*Digital Leaders*

4. CARACTERIZAÇÃO DA SITUAÇÃO DA INTELIGÊNCIA ARTIFICIAL NA ÁREA DA DEFESA

Neste capítulo, procede-se ao estudo de ambiente interno recorrendo a análises de natureza qualitativa e quantitativa, baseadas em consulta documental e num questionário de diagnóstico de MIA.

4.1. A INTELIGÊNCIA ARTIFICIAL NAS FORÇAS ARMADAS

Ao nível das FA foi identificada a ausência de uma estratégia específica e autónoma para a IA, assim como para a TD ou para os Dados, mas verifica-se a existência de estratégias e iniciativas conexas com a IA, designadamente, no âmbito da Inovação e das TED.

É o caso Diretiva Estratégica para a Inovação nas Forças Armadas (EMGFA, 2022). Adicionalmente, a Diretiva Estratégica do EMGFA 2023-2026, também contempla linhas de ação que habilitam à adoção de ferramentas de IA e de uma infraestrutura tecnológica focalizada em dados e análise de dados que pode ser potenciada pela utilização de ferramentas de IA na formulação da informação e na criação do conhecimento (EMGFA, 2023). Por fim, no âmbito da resposta ao questionário de MIA, o EMGFA reconhece a necessidade de estratégias específicas e autónomas para a TD e para a IA, bem como a criação duma nova estrutura orgânica dedicada a esta temática, pois a transversalidade da aplicação da IA não é consentânea com uma organização fortemente estruturada e rígida.

Destaca-se também, a estratégia para as TED da Marinha onde assume especial relevância a edificação de capacidades *Big Data* e de IA para o seu emprego em contexto operacional e transversalmente nas atividades não operacionais na Marinha, em particular na área da manutenção, do abastecimento e no âmbito do funcionamento das Unidades, Estabelecimentos e Órgãos (Marinha, 2024).

O Exército produziu orientações estratégicas para a Inovação, contemplando aspetos que envolvem as TED, desmaterialização de processos e digitalização (Exército, 2022). Mais recentemente, a Diretiva Para a Investigação, Desenvolvimento e Inovação no Exército identifica os sistemas de IA como uma

prioridade tecnológica (Exército, 2024). Em sede de resposta ao questionário de MIA, o Exército referiu que se encontra a desenvolver vários projetos com integração de IA, bem como está a elaborar uma estratégia para a IA, sugerindo a adoção de uma infraestrutura de suporte à IA *on-premise* ao nível da Defesa, por motivos de segurança e económicos.

A Força Aérea também desenvolveu orientações estratégicas para a transição digital, para a eficiência nos processos e para a formação digital dos recursos humanos (Força Aérea, 2022). Em sede de resposta ao questionário de MIA, a Força Aérea referiu que, não obstante a situação atual no que respeita à MIA, tem desenvolvido esforços no sentido de ganhar capacidade de IA, designadamente, a Divisão de Inovação e Transformação Organizacional do Estado-Maior da Força Aérea encontra-se a desenvolver uma estratégia e política para a IA.

Releva-se ainda a existência de centros de experimentação na Marinha e no Exército, designadamente, o Centro de Experimentação Operacional da Marinha (CEOM), a Célula de Experimentação Operacional de Veículos Não Tripulados (CEOV) da Marinha e o Centro de Experimentação e Modernização Tecnológica do Exército (CEMTex), que se constituem como facilitadores do desenvolvimento tecnológico e inovação.

4.2. A inteligência artificial nas autoridades nacionais

A AAN e a AMN não desenvolveram estratégias específicas, autónomas, para a IA, nem TD ou Dados.

No âmbito da resposta ao questionário de MIA, a AAN identificou algumas áreas onde a utilização da IA poderá trazer vantagens: gestão de movimentos aeroportuários, espaço aéreo, tráfego aéreo e operações aéreas militares. Por seu lado, a AMN destacou a potencial utilidade da IA no combate à criminalidade que está cada vez mais sofisticada a nível tecnológico e a criação do Núcleo de Inovação e Desenvolvimento Tecnológico, da Direção-Geral da Autoridade Marítima, em abril de 2022.

4.3. A inteligência artificial nos serviços centrais do ministério da defesa nacional

Os Serviços Centrais do MDN não desenvolveram estratégias específicas, autónomas, para a IA, contudo foi possível verificar a existência de várias iniciativas relacionadas com a implementação da IA na área da Defesa.

Na sua resposta ao questionário de MIA, a SGMDN mencionou ter a expectativa de utilizar a IA para potenciar a Inovação, promover a TD do MDN e responder às atuais necessidades organizacionais, designadamente nas diversas áreas funcionais (Recursos Humanos, Financeira e Logística). Identificou desafios na implementação de plataformas tecnológicas (maioritariamente *Cloud*) decorrentes da necessidade de cumprimento da legislação vigente, a necessidade de contratar ou formar talento na área da IA e dificuldades na contratação de serviços tecnológicos.

Em sede de questionário, a DGRDN mencionou que no âmbito das suas competências como entidade coordenadora da representação internacional ao nível da Defesa, tem acompanhado e participado nas iniciativas da OTAN e da Agência de Defesa Europeia relativas às estratégias e respetivos planos de ação sobre a IA na Defesa. Estas iniciativas suportam futuros desenvolvimentos na Defesa, em geral, e na DGRDN em particular, designadamente no plano estratégico, parcerias e inovação no âmbito do desenvolvimento, adoção e utilização de IA.

A DGPDN, em resposta ao questionário de MIA, referiu que Portugal subscreveu várias iniciativas internacionais no âmbito da utilização responsável da IA.

4.4. A ineligência artificial na idD Portugal Defence, S.A. e empresas participadas

A idD e empresas participadas não desenvolveram estratégias específicas, autónomas, para a IA.

Na resposta ao questionário a idD releva o papel cada vez mais importante da IA na área da Defesa, tendo realçado a necessidade das estratégias de defesa de IA incorporarem as questões éticas, legais e de segurança, bem como o respeito dos direitos humanos e das leis internacionais, designadamente o *AI Act* da UE. A idD reconhece que se encontra numa fase preliminar de adoção da IA admitindo que, após a publicação e entrada em vigor da regulamentação europeia referida, será mais fácil o desenvolvimento de uma estratégia para utilização da IA nas organizações e na própria idD.

Em sede de questionário de MIA, a AA referiu que no contexto da "Academia Arsenal" e em particular do seu Centro de Inovação e Experimentação inovAA tem desenvolvido várias iniciativas, parcerias, provas de conceito e projetos no contexto

da TD e sua integração nos processos de engenharia. Assim, a AA tem procurado desenvolver projetos com empresas, universidade e entidades para procurar testar casos de uso real e avaliar o retorno do investimento dos mesmos.

A AA mencionou também que, atenta a sua missão principal de prestar serviços à Marinha Portuguesa, tem procurado desenvolver estes projetos sempre de forma integrada o mais possível com a Marinha, pois o processo de reparação/manutenção/modernização, inicia-se e termina na Marinha.

A OGMA reconhece que a utilização da IA na empresa é incipiente. Não obstante, a OGMA acredita que existe potencial de utilização da IA, em algumas áreas da Empresa, por exemplo nas engenharias de produto ou processo.

A Edisoft, referiu que está mais envolvida em casos concretos de *Machine Learning* para resolver problemas específicos, em especial no controlo de tráfego aéreo.

Na resposta ao questionário, a EID evidenciou que, no âmbito dos sistemas militares, a doutrina de referência da OTAN e UE apresenta elevada volatilidade, sendo difícil para a indústria acompanhar os requisitos.

4.5. Diagnóstico de Maturidade Digital

Para aferir o nível de MIA da área da Defesa, foi aplicado o diagnóstico de MIA, apresentado no segundo capítulo, através da utilização de um questionário estruturado com 20 perguntas fechadas de resposta única e obrigatória destinadas a determinar o nível de MIA da organização sobre a IA e uma questão aberta no intuito de dar oportunidade à organização respondente de partilhar as suas perspetivas sobre a IA. Obtiveram-se 16 respostas não probabilísticas voluntárias dos organismos da área da Defesa.

Importa salientar que presente estudo assume o pressuposto de que a avaliação que cada organismo apresentou sobre o respetivo nível de MIA, corresponde à situação efetiva da MIA no mesmo[4].

Da análise efetuada verifica-se que o **nível global de maturidade nas diversas dimensões do MMIA é mínimo**, correspondendo ao nível de maturidade "Nível 1 – Inicial", com moda e mediana de 1. As figuras 4 e 5 exibem as frequências absolutas e relativas percentuais dos níveis de MIA relativamente à globalidade das dimensões.

[4] Ressalva-se que, dado o constrangimento de tempo e de recursos humanos para a realização do presente estudo, não se procedeu à recolha e análise das evidências mencionados no questionário de MIA.

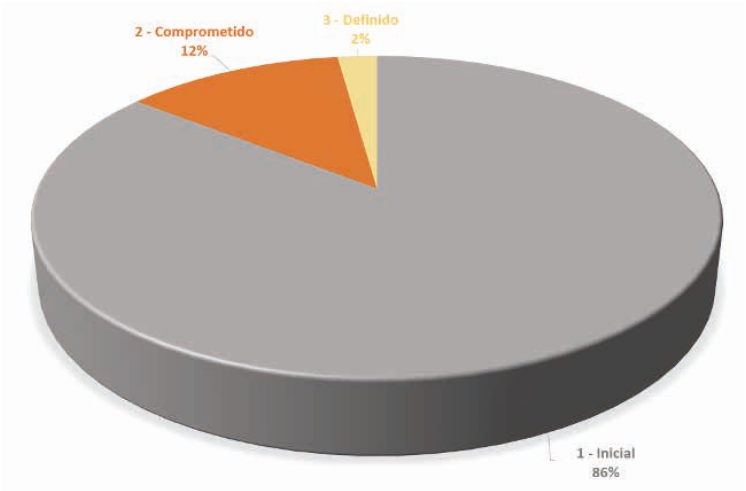

Figura 5 – Gráfico circular da frequência relativa percentual do Nível de MIA

Por outro lado, a análise estatística descritiva efetuada permite evidenciar que não existem diferenças substanciais de MIA entre os diversos organismos da área da Defesa, apurando-se que, quer a moda quer a mediana apresentam de forma geral o valor mínimo, ou seja 1, o que corresponde ao "Nível 1 – Inicial", sem prejuízo de se observarem pontualmente níveis de MIA mais elevados.

4.6. Síntese conclusiva e resposta à Questão Derivada 2

Da análise efetuada, confirma-se a inexistência de estratégias específicas e autónomas para a IA. Não obstante este facto, as FA são unânimes quanto à importância da integração da IA nas suas operações e atividades, verificando-se várias iniciativas de desenvolvimento de estratégias relacionadas com esta área.

Assim, verifica-se a inclusão de objetivos e linhas de ação relativos à IA em diversos documentos estratégicos das FA, relevando-se a "Diretiva Estratégica para a Inovação nas Forças Armadas" do EMGFA que procura coordenar os esforços dos ramos no âmbito da Inovação, para a qual as TED em geral e a IA em particular muito podem contribuir.

Destaca-se a Diretiva 07/CEMA/2024 da Marinha, relativa às TED (2024), a qual inclui objetivos estratégicos e linhas de ação dedicados à IA e ao *Big Data*, para o seu emprego em contexto operacional e transversalmente nas atividades não

operacionais na Marinha, em particular na área da manutenção, do abastecimento e no âmbito do funcionamento das Unidades, Estabelecimentos e Órgãos.

Importa também referir a existência de centros de experimentação na Marinha e no Exército e que outros organismos da área da Defesa têm um forte interesse na adoção e utilização da IA, tendo desenvolvido várias iniciativas no sentido da utilização da IA, destacando-se a SGMDN e a AA.

Adicionalmente, foi identificada a necessidade de se definir uma estrutura transversal às organizações da área da Defesa, para a liderança e condução do processo de governação atinente à implementação duma estratégia para o desenvolvimento, adoção e utilização da IA, bem como de se disponibilizar uma plataforma/infraestrutura tecnológica, desejavelmente *on-premise*, transversal ao MDN para suporte do edifício da IA.

A análise documental e o questionário de MIA permitiram apurar que as diversas entidades que integram a área da Defesa, encontram-se num nível global de MIA "Nível 1 – Inicial" podendo alguns organismos em determinadas dimensões exibir elementos relacionados com níveis de MIA mais elevados, "Nível 2 – Comprometido" e "Nível 3 – Definido".

Da análise da legislação, documentação estratégica e das respostas à questão 21 do questionário de MIA, foi possível identificar as potencialidades, que correspondem a boas práticas, iniciativas, infraestruturas e características específicas das organizações da área da Defesa, que lhes conferem vantagens competitivas.

Tabela 7 – Potencialidades

	Oportunidades	Fonte
P1	Existência de infraestruturas de ensino, formação, experimentação/ investigação e treino nas FA	Questionário/Diretivas Estratégicas
P2	Empenho das lideranças das FA e de outros organismos da área da Defesa na integração da IA nas capacidades militares e na gestão da organização	Questionário/Diretivas Estratégicas /Legislação
P3	Existência de Gestão Estratégica com controlo nas FA e definição de objetivos estratégicos no âmbito da IA	*Diretivas Estratégicas*
P4	Existem iniciativas de IA e uma cultura de inovação nas FA e noutros organismos da área da Defesa	Questionário/Diretivas Estratégicas
P5	Existência duma relação privilegiada entre a Base Tecnológica e Industrial de Defesa e a área da Defesa	*Questionário/Diretivas Estratégicas*

Tabela 8 – Vulnerabilidades

	Ameaças	Fonte
V1	Inexistência de liderança, estrutura organizacional, processo de governação e controlo, transversais e exclusivamente dedicados à IA	*Questionário*
V2	Não se encontra assegurada a utilização Responsável, Governável e Contestável da IA	*Questionário*
V3	Inexistência duma estratégia para o desenvolvimento, adoção e utilização da IA de forma transversal à área da Defesa	Questionário
V4	Não está assegurada a disponibilidade do talento necessário para o desenvolvimento, adoção e utilização da IA	*Questionário*
V5	Não estão asseguradas as infraestruturas/plataformas tecnológicas, nem uma arquitetura comum de dados fiáveis, de suporte à IA	*Questionário*
V6	Inexistência duma cultura data-driven, adaptativa, tolerante ao risco, de experimentação, melhoria contínua e iterativa	*Questionário*

5. FORMULAÇÃO DE CONTRIBUTOS PARA A DEFINIÇÃO DUMA ESTRATÉGIA DE INTELIGÊNCIA ARTIFICIAL NA ÁREA DA DEFESA

Neste capítulo, decorrente das análises anteriores e através de raciocínio crítico são apresentados os contributos para a elaboração de uma estratégia e assim responder à QC.

5.1. Análise SWOT

Para definir os objetivos estratégicos, foi realizada uma análise SWOT (Figura 6) para perceber como os fatores externos: Oportunidades e Ameaças se relacionam com os fatores internos: Potencialidades e Vulnerabilidades (Ribeiro & Pinto, 2022).

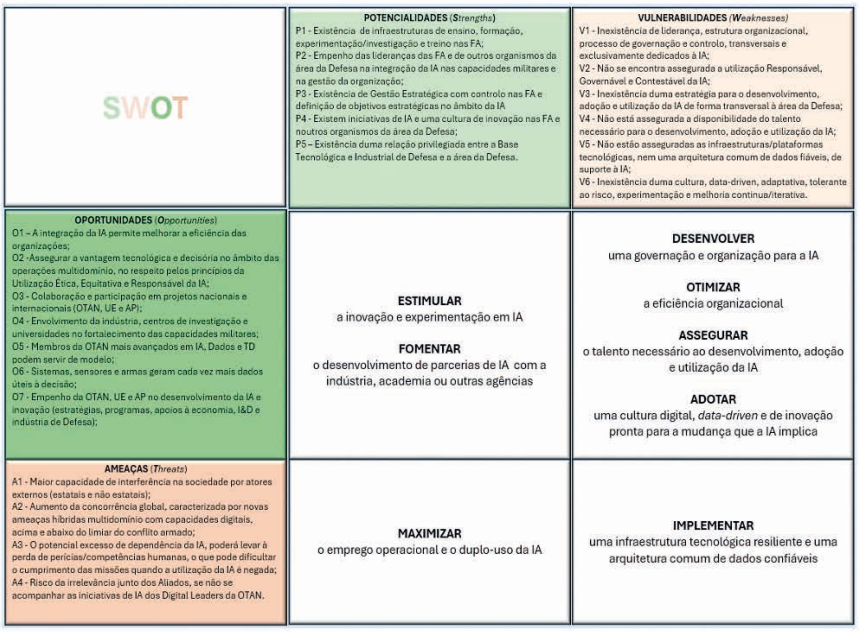

Figura 6 – Análise SWOT

5.2. Contributos para uma estratégia de inteligência artificial na área da Defesa

No capítulo precedente foi evidenciada a inexistência de uma estratégia para o desenvolvimento, adoção e utilização da IA na área da Defesa, pelo que se procurará apresentar contributos que permitam a sua elaboração.

Atenta a situação atual da MIA na área da Defesa, bem como o horizonte temporal estabelecido na Diretiva Estratégica para a Inovação nas Forças Armadas que inclui objetivos no âmbito da IA apresenta-se, como contributo, uma proposta do que poderá constituir uma visão simplificada do MDN, para o desenvolvimento, adoção e utilização da IA na área da Defesa até 2032: Em 2032, alcançaremos uma capacidade de autonomia estratégica em IA que garantirá o respeito dos aliados e reforçará a nossa posição no cenário global.

O desenvolvimento, adoção e utilização da IA, requer a disponibilidade de meios financeiros, talento, dados confiáveis e acessíveis, processos digitais e tecnologia.

As orientações estratégicas têm a finalidade de direcionar e orientar o esforço principal da formulação estratégica. Normalmente, num mapa da estratégia (Figura

7), representam-se na vertical, agregando objetivos das perspetivas genética, estrutural e operacional (Ribeiro & Pinto, 2022). Com base num raciocínio lógico, a partir do conhecimento acumulado, estabelecem-se três orientações estratégicas:

- **Promover o Talento e Cultura para o desenvolvimento, adoção e utilização da Inteligência Artificia**l – Gerar e reter o talento necessário, com conhecimentos profundos de IA e áreas conexas, bem como adotar uma cultura digital orientada para os dados, de experimentação contínua e de tolerância ao erro como parte dum processo iterativo de inovação e melhoria continua das soluções.
- **Fomentar a colaboração e a transversalidade para o desenvolvimento, adoção e utilização da Inteligência Artificial** – Desenvolver a governação e a organização para a IA, através de uma liderança para a IA, estabelecendo normas, processos e estruturas transversais à área da Defesa. Fomentar parcerias de IA com a indústria, academia ou outras agências bem como colaborar estreitamente com aliados e parceiros, de forma a acelerar a capacidade de inovação e experimentação em IA.
- **Fomentar a utilização da Inteligência Artificial desde a Retaguarda até à Frente de Batalha** – A utilização responsável da IA deve permitir a vantagem operacional, a interoperabilidade com os Aliados e a eficiência da organização. Para o efeito são necessárias infraestruturas tecnológicas adequadas, seguras e resilientes, bem como o acesso seguro e em tempo útil a dados confiáveis.

Figura 7 – Mapa da estratégia elaborado a partir da análise SWOT
Fonte: Adaptado a partir de Ribeiro e Pinto (2022).

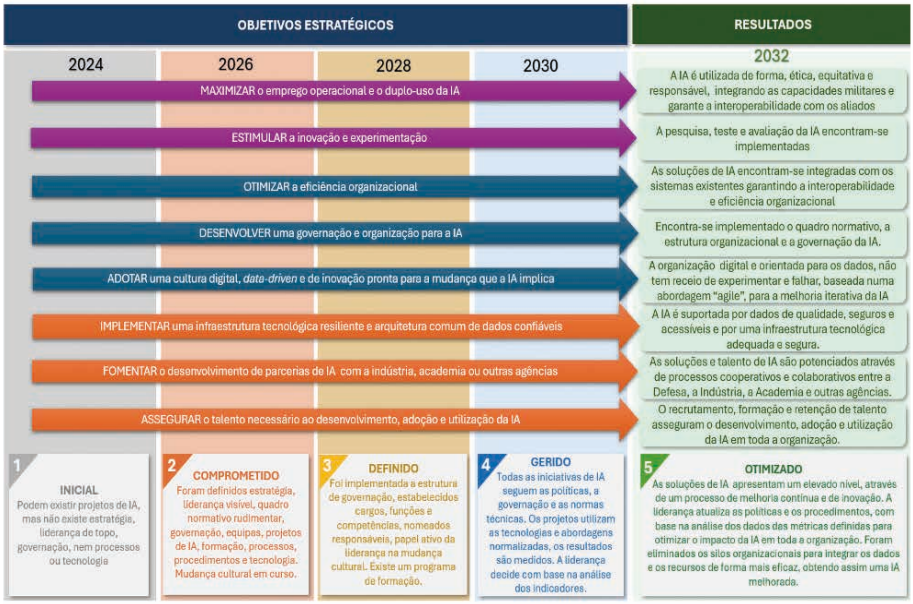

Figura 8 – Roteiro para o desenvolvimento, adoção e utilização da IA até 2032
Fonte: Adaptado do modelo de Maturidade em IA da Mitre Corporation (2023).

Recorrendo ao mapa da estratégia (Figura 7) e raciocínio lógico (Santos & Lima, 2019, p. 19) e com base nas soluções identificadas pelos *Digital Leaders* e do caráter prescritivo do MMIA utilizado, desenvolveram-se os Objetivos Estratégicos (OE) e as Linhas de Ação (LA) constantes no Quadro 8.

Quadro 8 – Objetivos Estratégicos e Linhas de Ação

OE.01	**Assegurar o talento necessário ao desenvolvimento, adoção e utilização da IA**: Este objetivo visa garantir as necessidades de pessoal, com as devidas qualificações, para o desenvolvimento, adoção e utilização da IA.	
	LA.01.01	**Edificar e gerir a Força de Trabalho de IA:** definição de uma carreira de IA e de um chefe de classe profissional; criação de cargos e definição das respetivas competências; identificar e empregar o talento existente e; assegurar o recrutamento, formação e retenção do talento necessário ao desenvolvimento, adoção e utilização da IA.
	LA.01.02	**Promover parcerias académicas e o intercâmbio:** Aproveitar as intervenções apoiadas pelo governo ao nível dos melhores talentos, dos doutoramentos e dos mestrados (designadamente bolsas e estágios na área da Defesa). Encorajar o intercâmbio entre a Defesa, o meio académico e o sector tecnológico, estabelecendo mecanismos expeditos de colocação para líderes talentosos no domínio da IA.
OE.02	**Fomentar o desenvolvimento de parcerias de IA com a indústria, academia ou outras agências:** Este objetivo pretende fomentar a colaboração em rede entre a Defesa, a Academia e a Indústria, procurando-se sinergias focadas em parcerias nacionais e internacionais, incluindo a cooperação no âmbito da OTAN e UE, para o desenvolvimento, adoção e utilização da IA	
	LA.02.01	**Fomentar parcerias:** A IA é uma tecnologia eminentemente de dupla utilização, implicando a estrita interação da Defesa com o sector civil, tanto industrial como académico. Assim, devem ser exploradas e maximizadas as parcerias intergovernamentais, académicas, industriais e com outras agências, nacionais e internacionais, para permitir o rápido desenvolvimento, adoção e utilização de IA.
	LA.02.02	**Trabalhar em estreita colaboração com aliados e parceiros:** O caminho mais rápido para dominar estas tecnologias é trabalhar em estreita colaboração com aliados e parceiros, designadamente, no âmbito da OTAN e UE, mas não só, reforçando a comunicação e interoperabilidade de dados, software e sistemas.
OE.03	**Implementar uma infraestrutura tecnológica resiliente e uma arquitetura comum de dados confiáveis:** Este objetivo visa dotar a organização com uma plataforma/infraestrutura tecnológica para apoio ao desenvolvimento, integração e funcionamento de soluções de IA, bem como, desenvolver uma arquitetura comum de dados, garantindo a governação, a privacidade, a segurança e acessibilidade dos mesmos.	
	LA.03.01	**Assegurar infraestruturas/plataformas tecnológicas de IA resilientes:** Disponibilizar infraestruturas/plataformas tecnológicas resilientes, interoperáveis e transversais à área da Defesa (ambiente de cálculo, armazenamento, transferência de dados e sistemas de apoio), modernizar as infraestruturas de C5ISR e proteger as redes, aplicações, ativos e serviços através duma abordagem de cibersegurança "Zero Trust".
	LA.03.02	**Edificar o "*Digital Backbone*" da Defesa:** Um "ecossistema" que combina pessoas, processos, dados e tecnologia. Com o apoio de uma cibersegurança reforçada, as tecnologias serão atualizadas, a força de trabalho será transformada digitalmente e serão implementados processos sólidos para garantir a coerência e normas comuns.
	LA.03.03	**Reconhecer que os dados são um ativo estratégico:** Definir e implementar uma Estratégia de Dados, para garantir o acesso seguro a dados confiáveis, bem governados, com uma arquitetura adequada e devidamente classificados, o que assenta no controlo do ciclo de vida dos dados, desde a geração até à valorização, incluindo a produção, o processamento e o armazenamento em grande escala.

[Cont.]

	LA.03.04	**Organização orientada para os dados (*Data-Driven*):** Pretende-se acabar com os silos digitais; estabelecer arquiteturas de dados, normas, convenções de rotulagem e plataformas de exploração comuns (incluindo um ambiente operacional de análise de IA); promover o acesso autorizado a dados integrados de um *Data Warehouse* da Defesa.
OE.04	**Adotar uma cultura digital, *data-driven* e de inovação pronta para a mudança que a IA implica:** Este objetivo procura assegurar a existência de normas e valores organizacionais que apoiam uma cultura adaptativa e tolerante ao risco que está pronta aceitar os tipos de mudanças que a IA pode implicar.	
	LA.04.01	**Promover a mudança cultural:** Através da adoção duma cultura de inovação, proativa, adaptativa, colaborativa, transversal, de segurança, orientada para os dados e "*agile*", ou seja, a Defesa deve adotar uma cultura de organização digital e orientada para os dados que não tem receio de experimentar e falhar, num processo contínuo e iterativo de melhoria da IA.
OE.05	**Desenvolver uma governação e organização para a IA:** Este objetivo procura identificar as ações a desenvolver para se estabelecer um conjunto alargado de políticas, normas, estruturas, processos e mecanismos de monitorização e controlo para se operacionalizar a gestão estratégica, estabelecer e implementar um modelo de governação e adaptar a estrutura organizacional atinentes ao desenvolvimento, adoção e utilização de IA.	
	LA.05.01	**Estabelecer a governação e estrutura organizacional do processo de implementação da Estratégia de IA:** Estabelecer a governação dos processos de implementação da estratégia de IA, designadamente através da nomeação de responsáveis, da criação duma estrutura central e transversal para o efeito e de mecanismos de controlo da execução da estratégia.
	LA.05.02	**Alocar financiamento aos investimentos em IA e Tecnologia:** Alocar financiamento aos investimentos em IA e Tecnologia, através da afetação do orçamento da Defesa e explorando programas/mecanismos de financiamento nacionais e internacionais.
	LA.05.03	**Criar um "Centro de IA da Defesa (CIAD)":** O qual terá as seguintes funções: Atuar como um núcleo visionário, liderando o desenvolvimento e a utilização da IA em toda a Defesa; capacitar e coordenar o rápido desenvolvimento, a entrega e a expansão de projetos de IA que conferem vantagem estratégica; fornecer acesso a serviços digitais/dados subjacentes ao ecossistema da Defesa e a fontes de especialização como serviços comuns a toda a Defesa (na maioria dos *Digital Leaders* encontra-se na direta dependência do Secretário de Estado da Defesa).
OE.06	**Otimizar a eficiência organizacional:** Realizar a transição digital dos processos, integrando sistemas de IA para otimizar operações, reduzir custos e impulsionar a eficiência organizacional.	
	LA.06.01	**Assegurar a utilização da IA na otimização da gestão:** através da TD e da utilização ética, equitativa e responsável IA, integrando plataformas de IA com sistemas existentes para garantir interoperabilidade e eficiência organizacional.
OE.07	**Estimular a inovação e a experimentação em IA** – Este objetivo visa garantir a implementação duma abordagem *agile* à inovação, assegurar que as práticas Humano-Máquina são aplicadas em soluções de IA e implementar a capacidade de Teste e Avaliação através da definição de processos, normas, governação e controlo.	
	LA.07.01	**Promover a Inovação em IA** – adotar uma abordagem "*agile*" de experimentação sistemática para iterar, lançar produtos mínimos viáveis, testar possibilidades, reduzir o risco das tecnologias e dos planos de formação, desenvolver novos conceitos e doutrinas operacionais e aumentar a apetência e capacidade para lançar inovações de IA a um ritmo acelerado.

[Cont.]

	LA.07.02	**Adotar uma abordagem Humano-Máquina** – A formação de equipas humano-máquina deverá constituir a abordagem por defeito para a adoção da IA, tanto por razões éticas e jurídicas como para concretizar o "efeito multiplicador" que advém da combinação da cognição e da inventividade humanas com as capacidades analíticas da velocidade das máquinas.
	LA.07.03	**Assegurar a capacidade de teste e garantia técnica e certificação** – Garantir que as novas capacidades de IA são seguras, robustas, eficazes e ciberseguras, devendo ser adotadas abordagens inovadoras em matéria de teste, avaliação, verificação e validação, estabelecendo novas capacidades de teste em ambiente real e virtual e colaborando com uma vasta gama de parceiros.
OE.08	**Maximizar o emprego operacional e o duplo-uso da IA** – Este objetivo pretende assegurar o desenvolvimento, a implementação, o funcionamento e a manutenção das capacidades baseadas em IA de modo eficaz e eficiente. As soluções de IA são implementadas e monitorizadas para atender ao uso pretendido.	
	LA.08.01	**Explorar a natureza de Duplo Uso da IA** – apoiando-se num ecossistema de dupla utilização, e aceder a capacidades de IA de interesse para a área da Defesa através da aquisição de software e suporte para estas soluções comerciais, libertando o talento da Defesa para desafios inerentemente militares.
	LA.08.02	**Monitorização das soluções de IA** – através da instrumentação e novas formas de recolher dados relevantes para a IA, exigindo que os produtos e serviços de software tenham a capacidade de disponibilizar dados de utilização e de desempenho.
	LA.08.03	**Assegurar a confiança do utilizador** – assegurando que: os utilizadores têm a formação, a compreensão e a experiência adequadas; mecanismos de ética, garantia e conformidade reconhecidos e; a verificação, validação e certificação permanentemente das capacidades de IA.
	LA.08.04	**Assegurar a interoperabilidade com os Aliados:** As soluções de IA integradas nas capacidades militares e de duplo-uso deverão assegurar a interoperabilidade com os aliados.
	LA.08.05	**Promover a Utilização Ética, Equitativa e Responsável da IA:** As soluções de IA integram os requisitos da utilização ética, equitativa e responsável da IA. Observar e participar no trabalho internacional sobre o uso responsável da IA, designadamente no âmbito da OTAN e UE, facilitando a colaboração e interoperabilidade.

As propostas do presente estudo encontram-se validadas. A larga maioria dos especialistas concorda que a proposta é adequada, exequível e aceitável (nível de aprovação superior a 80% para todas as iniciativas relativamente a cada uma das três provas da estratégia), mas foram manifestadas algumas reservas quanto à exequibilidade, sobretudo devido à falta de capacidade para recrutar e reter o talento necessário para esta transformação na área da Defesa. A generalidade dos especialistas considera que este estudo acrescentou conhecimento e que é útil para desenvolver e usar a Inteligência Artificial na área da Defesa e que aprenderam com o mesmo.

5.3. Síntese conclusiva e resposta à Questão Central

Com base nas respostas às QD foi feita uma análise SWOT, que permitiu a elaboração de um mapa da estratégia (Figura 7), um roteiro para o desenvolvimento, adoção e utilização da IA até 2032 (Figura 8), e a definição de OE e LA (Quadro 8).

Nesta sequência, tendo sido demonstrado que o nível de MIA na área da Defesa é mínimo, bem como a inexistência duma estratégia para o desenvolvimento, adoção e utilização da IA, os primeiros passos em direção a um nível otimizado de MIA (nível 5) começam com a criação da referida estratégia, por empenho do vértice estratégico, e da nomeação de um responsável pela sua implementação, ficando assim acautelada a liderança deste processo. Este responsável deve chefiar uma estrutura central do MDN de atuação transversal a toda a área da Defesa (à semelhança de outros *Digital Leaders* da OTAN), que deve ter competências para atuar como um núcleo visionário, liderando o desenvolvimento e a utilização da IA em toda a Defesa; capacitar e coordenar o rápido desenvolvimento, a entrega e a expansão de projetos de IA que conferem vantagem estratégica; fornecer acesso a serviços digitais/dados subjacentes ao ecossistema da Defesa e a fontes de especialização como serviços comuns a toda a Defesa.

A estratégia procura empregar os meios (pessoas, dados, processos e tecnologia) atingir os fins (a otimização do funcionamento da organização e a prevalência nas operações multidomínio). Assim, na perspetiva genética foram definidos três objetivos estratégicos: assegurar o talento necessário ao desenvolvimento, adoção e utilização da IA; fomentar o desenvolvimento de parcerias de IA com a indústria, academia ou outras agências; implementar uma infraestrutura tecnológica resiliente e uma arquitetura comum de dados confiáveis. No âmbito estrutural, foram definidos três objetivos estratégicos: Adotar uma cultura digital, *data-driven* e de inovação pronta para a mudança que a IA implica; desenvolver uma governação e organização para a IA; otimizar a eficiência organizacional. Na perspetiva operacional, foram definidos dois objetivos estratégicos: Estimular a inovação e experimentação; maximizar o emprego operacional e o duplo-uso da IA.

6. CONCLUSÕES

O mundo atual caracteriza-se por uma fortíssima competição estratégica, onde os principais atores procuram assegurar o máximo de vantagens possíveis e negar as mesmas aos adversários, efetivos ou potenciais, em todas as áreas e

em todos os domínios. Uma dessas áreas é a tecnologia e procura-se a vantagem tecnológica a um ritmo nunca antes visto, especialmente no âmbito das TED. Entre estas tecnologias assume especial relevância a IA, a qual face ao crescimento exponencial dos dados disponibilizados pelo número crescente de sensores e plataformas tecnológicas de informação, assume-se como uma ferramenta incontornável para permitir que a decisão humana tenha em consideração a informação resultante dos dados disponíveis.

No âmbito das FA, atento o crescimento exponencial dos dados a processar, resultante da complexidade tecnológica dos meios utilizados e do cada vez maior número de domínios onde as operações decorrem, torna-se imprescindível e da maior urgência e prioridade o desenvolvimento, adoção e utilização da IA. Esta é a única forma de as FA assegurarem a vantagem tecnológica e decisória face aos potenciais adversários, bem como maximizar a eficiência e eficácia, desde as atividades e processos administrativos e de suporte, até às operações no campo de batalha.

Neste trabalho foi seguido um procedimento metodológico baseado num processo de raciocínio dedutivo, tendo sido usada uma estratégia mista, assente num estudo de caso.

A análise qualitativa baseou-se em entrevistas e documentação relevante. A análise quantitativa decorreu da aplicação de um questionário de IA, respondido por 16 organismos representativos da área da Defesa.

Desta forma, foi possível observar que na OTAN, os *Digital Leaders* (EUA, Reino Unido, França, Espanha, Finlândia, Noruega e Canadá) já publicaram uma estratégia específica e autónoma para o desenvolvimento, adoção e utilização da IA na área da Defesa, ao contrário dos outros países-membros, onde se inclui Portugal. Verifica-se ainda que estes países, desenvolveram estratégias específicas e autónomas para áreas facilitadoras da IA, designadamente, TD e Dados e que, quase todos, estabeleceram uma estrutura central e transversal, dedicada à governação do processo de implementação da estratégia de IA, entre outras competências. O posicionamento organizacional desta estrutura, varia entre os aliados, podendo encontrar-se na dependência direta do Secretário de Estado da Defesa (EUA, Reino Unido e Noruega), da Direção-Geral do Armamento (França e Espanha) ou do Chefe das Forças Armadas (Finlândia).

A estratégia de IA da OTAN, aprovada em outubro de 2021 pelos ministros de defesa dos países-membros, reconhece que a IA está a alterar o ambiente global de defesa e segurança, constituindo-se como uma oportunidade para fortalecer

a vantagem tecnológica da OTAN, mas simultaneamente também aumentará a velocidade das ameaças que a mesma terá de enfrentar. No âmbito desta estratégia, relevam-se os princípios da utilização responsável da IA.

A UE publicou no corrente ano, um conjunto de medidas políticas para apoiar o desenvolvimento de IA confiável, as quais incluem o Pacote de Inovação de IA e o Plano Coordenado sobre IA, tendo também aprovado o projeto final do *AI Act*, que é o primeiro quadro jurídico de sempre em matéria de IA, abordando os riscos da IA e posicionando a Europa para desempenhar um papel de liderança a nível mundial.

Por seu turno, Portugal publicou em 2019 a sua iniciativa estratégica para a IA, tendo ainda um plano de ação e estratégias setoriais nomeadamente para a TD, dados, *Cloud*, computação avançada e cibersegurança.

A análise documental, as entrevistas e a avaliação de MIA permitiram apurar que as FA, Autoridades, Serviços Centrais do MDN e idD e empresas participadas apresentam, em termos globais, o nível mais baixo de MIA do MMIA adotado, ou seja, "Nível 1 – Inicial".

Entre as razões subjacentes a esta situação destacam-se lacunas no desenvolvimento de talentos, liderança, estratégia, governação, organização, processos digitalizados, dados confiáveis e plataformas tecnológicas (dados e computação).

Não obstante este facto, foi possível observar níveis de MIA superiores de algumas organizações em certas dimensões. Neste âmbito, relevam-se a publicação da estratégia de inovação do EMGFA, a diretiva estratégica para as TED da Marinha (que inclui objetivos estratégicos e linhas de ação para a IA e Big Data), os centros de experimentação da Marinha, do Exército e AA, projetos e casos de uso de IA do Exército e da SGMDN, e o "Programa de Digitalização de Processos de Engenharia" do centro de experimentação inovAA.

Atentas as evidências anteriormente enunciadas, podemos concluir que o principal contributo do presente trabalho de investigação para o conhecimento consiste na oportunidade do próprio tema, demonstrando-se que existe uma necessidade premente de se iniciar um programa liderado e governado centralmente pelo MDN, através da definição e implementação de uma estratégia e da criação duma estrutura dedicada ao desenvolvimento, adoção e utilização da IA, de modo transversal na área da Defesa.

Através da análise documental das estratégias da OTAN e dos *Digital Leaders* identificaram-se os princípios a observar num projeto alargado de desenvolvimento,

adoção e utilização de IA. Apresentou-se um modelo de diagnóstico de IA, com natureza prescritiva. Para a elaboração do mapa estratégico (Figura 7) com a identificação dos objetivos estratégicos (Quadro 8) utilizou-se uma análise SWOT. Foi ainda elaborado um roteiro para o desenvolvimento, adoção e utilização da IA, de acordo com o prescrito pelo MMIA adotado (Figura 8).

Nesta sequência, tendo sido demonstrado que o nível de MIA na área da Defesa é mínimo, bem como a inexistência duma estratégia específica e autónoma para o desenvolvimento, adoção e utilização da IA, os primeiros passos em direção a um nível otimizado de MIA (nível 5) começam com a criação da referida estratégia e da nomeação de um responsável pela sua implementação, ficando assim acautelada a liderança deste processo. Este responsável deve chefiar uma estrutura central de atuação transversal a toda a área da Defesa , na dependência do MDN (à semelhança dos *Digital Leaders* da OTAN), que deve ter competências para atuar como um núcleo visionário, liderando o desenvolvimento e a utilização da IA em toda a Defesa; capacitar e coordenar o rápido desenvolvimento, a entrega e a expansão de projetos de IA que conferem vantagem estratégica; fornecer acesso a serviços digitais/dados subjacentes ao ecossistema da Defesa e a fontes de especialização como serviços comuns a toda a Defesa.

Na perspetiva genética foram definidos três objetivos estratégicos: assegurar o talento necessário ao desenvolvimento, adoção e utilização da IA; fomentar o desenvolvimento de parcerias de IA com a indústria, academia ou outras agências; implementar uma infraestrutura tecnológica resiliente e uma arquitetura comum de dados confiáveis. No âmbito estrutural, foram definidos três objetivos estratégicos: Adotar uma cultura digital, data-driven e de inovação pronta para a mudança que a IA implica; desenvolver uma governação e organização para a IA; otimizar a eficiência organizacional. Na perspetiva operacional, foram definidos dois objetivos estratégicos: Estimular a inovação e experimentação; maximizar o emprego operacional e o duplo-uso da IA.

Considera-se fundamental para o sucesso desta estratégia: o empenhamento dos responsáveis das organizações da área da Defesa (FA, Serviços Centrais, Autoridades e idD e empresas participadas); a definição duma liderança de topo responsável pela sua implementação; a criação duma estrutura central e de atuação transversal do MDN que deve ser um par dos restantes organismos da área da Defesa (possivelmente, na dependência do Secretário de Estado da Defesa Nacional, à semelhança dos *Digital Leaders* da OTAN), e que deve ter competências

para liderar e governar o desenvolvimento, adoção e utilização da IA em toda a Defesa; o desenvolvimento duma força de trabalho competente e; assegurar a disponibilidade das plataformas tecnológicas que suportam a IA e os Dados.

Pretende-se em última análise garantir que até 2032, em alinhamento com a Diretiva Estratégica para a Inovação nas Forças Armadas, a área da Defesa alcance uma capacidade de autonomia estratégica em IA, que garantirá o respeito dos aliados e reforçará a posição nacional no cenário global.

Assim, a recomendação deste estudo é que seja concebida e publicada uma estratégia de IA para a área da Defesa, ao nível mais elevado e transversal, de modo a garantir o alinhamento estratégico de todas as organizações da área da Defesa.

Não foram identificadas limitações ao desenvolvimento do presente estudo, mas verificou que se trata de uma temática de elevada complexidade.

Quanto a estudos futuros, havendo muitas áreas para explorar, avançam-se algumas sugestões que se encontram relacionadas com o objeto do presente estudo: Contributos para uma estratégia de dados na área da Defesa; Contributos para a governação e organização da IA na área da Defesa; Contributos para a edificação duma carreira na área digital, dados e IA; Estudo das plataformas tecnológicas de suporte à IA mais adequadas à área da Defesa; A adoção de uma nova cultura de inovação "*agile*" na área da Defesa.

Este estudo conclui que a importância estratégica que os líderes mundiais têm atribuído à IA é justificada, sendo crucial a sua exploração para garantir a credibilidade e relevância da área da Defesa junto da nação e dos aliados e parceiros.

REFERÊNCIAS BIBLIOGRÁFICAS

Alsheiabni, S., Cheung , Y., & Messom , C. (2019, junho). *Towards An Artificial Intelligence Maturity Model: From Science Fiction To Business Facts. Paper apresentado na Twenty-Third Pacific Asia Conference on Information Systems d*a Association for Information Systems, China. Retirado de https://core.ac.uk/download/pdf/301391799.pdf

Cable News Network. (2017). Who Vladimir Putin thinks will rule the world [Página *online*]. Retirado de https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html

Canadian Armed Forces. (2022). *Canadian Armed Forces Digital Campaign Plan* [Página *online*]. Retirado de https://www.canada.ca/en/department-

national-defence/corporate/reports-publications/canadian-armed-forces-digital-campaign-plan.html

CCDCOE. (2021). *Artificial Intelligence and Autonomy in the Military: An Overview of NATO Member States Strategies and Deployment*. Retirado de https://ccdcoe.org/uploads/2021/12/Strategies_and_Deployment_A4.pdf

Comissão Europeia. (2018). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões: Inteligência artificial para a Europa*. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52018DC0237

Comissão Europeia. (2024). Shaping Europe's digital future [Página *online*]. Retirado de https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

Conselho para as Tecnologias de Informação e Comunicação na Administração Pública. (2020). *Estratégia Cloud para a Administração Pública em Portugal*. Retirado de https://bo.tic.gov.pt/api/assets/etic/6a573aa2-f87d-4958-92c9-0f1de7b3bf63/

Correia, A. J. D. (2023). *A Transformação Digital nas Forças Armadas Portuguesas* (Trabalho de Investigação Individual do Curso de Promoção a Oficial General). Instituto Universitário Militar [IUM], Pedrouços.

Defesa Nacional. (s.d.). Organização [Página *online*]. Retirado de https://www.defesa.gov.pt/pt/defesa/organizacao/Paginas/default.aspx

Department of Defense. (2018). *Summary of the 2018 Department of Defense Artificial Intelligence Strategy - Harnessing AI to Advance Our Security and Prosperity*. Retirado de https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

Department of Defense. (2022). *DoD Zero Trust Strategy*. Retirado de https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

Department of Defense. (2022). *Responsible Artificial Intelligence Strategy and Implementation Pathway*. Retirado de https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF

Department of Defense. (2023). *Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage*. Retirado de https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALY TICS_AI_ADOPTION_STRATEGY.PDF

Department of Nacional Defence and Canadian Armed Forces. (2024). *The Department of Nacional Defence and Canadian Armed Forces Artificial*

Intelligence Strategy [Página *online*]. Retirado de https://www.canada.ca/en/department-national-defence/corporate/reports-publications/dnd-caf-artificial-intelligence-strategy.html

DigiChina. (2017). *Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)* [Página *online*]. Retirado de https://digichina.stanford.edu/work/full-translation-chinas-new-generation-artificial-intelligence-development-plan-2017/

Element AI. (2020). *The AI Maturity Framework*. Retirado de https://s3.amazonaws.com/external_clips/3430107/AI-Maturity-Framework_White-Paper_EN.pdf?1589551996

EMGFA. (2022). *Diretiva Estratégica para a Inovação nas Forças Armadas*. Retirado de https://www.emgfa.pt/pt/inovacao/Documents/Documentacao/DIR%20ESTRATEGICA%20INOVACAO%20FORCAS%20ARMADAS%2022_32_pt_21.03.2022.pdf

EMGFA. (2023). *Diretiva Estratégica do Estado-Maior-General das Forças Armadas 2023-2026*. Retirado de https://www.emgfa.pt/pt/inovacao/Documents/Documentacao/Diretiva%20Estrat%C3%A9gica%20EMGFA%202023%20-%202026.pdf

Executive Order 13859, February 11 (2019). *Maintaining American Leadership in Artificial Intelligence*. Federal Register, 3 C.F.R., 84(31), 3967-3972. Washington, DC: The White House. Retirado de https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf

Exército. (2022). *Estratégia de Inovação do Exército*. Retirado de https://assets.exercito.pt/SiteAssets/GabCEME/Inovar/Imagens%20Site%20Exercito/Estrat%C3%A9gia%20de%20Inova%C3%A7%C3%A3o%20do%20Ex%C3%A9rcito.pdf

Exército. (2024). *Diretiva N.º 42/CEME/2024, de 22 de fevereiro de 2024, Diretiva Para a Investigação, Desenvolvimento e Inovação no Exército*. Retirado de https://academiamilitar.pt/images/site_images/centro_investigacao/DIRT_N.%C2%BA_42CEME24_-_DIRETIVA_PARA_A_INVESTIGA%C3%87%C3%83O_DESENVOLVIMENTO_E_INOVA%C3%87%C3%83O_NO_EX%C3%89RCITO.pdf

Faculdade de Ciências e Tecnologia da Universidade Nova de Lisboa. (2022). No que consiste a metodologia Agile? [Página *online*]. Retirado de https://execed.fct.unl.pt/consiste-a-metodologia-agile/

Finnish Ministry of Defence. (2020). *Strategic Guidelines for Developing AI Solutions*. Retirado de https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162372/Strategic_guidelines_for_developing_ai_solutions.pdf?sequence=1&isAllowed=y

Força Aérea. (2022). *Diretiva Estratégica da Força Aérea 2022-2025*. Retirado de https://www.emfa.pt/paginas/fap/ficheiros/noticias/2023/Planeamento%20Estrategico%2022-25.pdf

Forsvarsdepartementet. (2023). *Strategi for kunstig intelligens for forsvarssektoren*. Retirado de https://kudos.dfo.no/documents/53467/files/34874.pdf

Fukas, P., Rebstadt , J., Remark , F., & Thomas, O. (2021). *Developing an Artificial Intelligence Maturity Model for Auditing*. Retirado de https://www.researchgate.net/publication/352192517_Developing_an_Artificial_Intelligence_Maturity_Model_for_Auditing

Fundação para a Ciência e Tecnologia. (2023). *Advanced Computing Portugal 2030*. Retirado de https://rnca.fccn.pt/wp-content/uploads/2023/01/advanced-computing-portugal_2030-acp-2030-relatorio.pdf

Gartner. (2020). Artificial Intelligence Maturity Model. Retirado de https://www.gartner.com/en/documents/3982174

Gartner. (s.d.). Big Data [Página *online*]. Retirado de https://www.gartner.com /en/information-technology/glossary/big-data

Google. (s.d.). O que é a segurança de confiança zero? [Página *online*]. Retirado de https://cloud.google.com/learn/what-is-zero-trust?hl=pt-br

Hill, M. M., & Hill, A. (2008). *Investigação por Questionário* (2ª Edição Ed.). Lisboa: Edições Sílabo.

House of Representatives. (2020). *National Artificial Intelligence Initiative Act of 2020*. Retirado de https://www.congress.gov/116/bills/hr6216/BILLS-116hr6216ih.pdf

IBM. (2021). *AI maturity framework for enterprise applications*. Retirado de https://www.ibm.com/downloads/cas/OB8M18WR

Leino, S.-P., Kuusisto, O., Paasi, J., & Tihinen, M. (2017). *VTT Model of Digimaturity. In Towards a new era in manufacturing: final report of VTT's for industry spearhead programme*. Retirado de https://publications.vtt.fi/pdf/technology/2017/T288.pdf

Marinha. (2024). *Diretiva 07/CEMA/2024, de 18 de março de 2024, Tecnologias Emergentes Disruptivas*. Lisboa: Autor.

Mathias, L. (2022). Mindminers Blog - Quais são os principais tipos de perguntas para questionário de pesquisa? [Publicação em blogue]. Retirado de https://mindminers.com/blog/tipos-de-perguntas-usados-em-questionarios/

McCarthy, J. (2007). *What is Artificial Intelligence?*. Retirado de https://www-formal.stanford.edu/jmc/whatisai.pdf

Microsoft. (2018). *AI Maturity and organizations - Understanding AI maturity*. Retirado de https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4DIvg

Ministére des Armées. (2019). *Artificial Intelligence in Support of defence*. Retirado de https://www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf

Ministry of Defence. (2022). *Defence Artificial Intelligence Strategy*. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1082416/Defence_Artificial_Intelligence_Strategy.pdf

MITRE Corporation. (2023). *The MITRE AI Maturity Model and Organizational Assessment Tool Guide: A Path to Successful AI Adoption*. Retirado de https://www.mitre.org/sites/default/files/2023-11/PR-22-1879-MITRE-AI-Maturity-Model-and-Organizational-Assessment-Tool-Guide.pdf

National Institute of Standards and Technology. (2020). *Zero Trust Architecture*. Retirado de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

OCDE. (2021). *An overview of national AI strategies and policies*. Retirado de https://goingdigital.oecd.org/data/notes/No14_ToolkitNote_AIStrategies.pdf

OCDE. (2023). How countries are implementing the OECD Principles for Trustworthy AI [Página *online*]. Retirado de https://oecd.ai/en/wonk/national-policies-2

OTAN. (2005). NATOTerm The Official NATO Terminology Database [Página *online*]. Retirado de https://nso.nato.int/natoterm/Web.mvc

OTAN. (2021). Summary of the NATO Artificial Intelligence Strategy [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_187617.htm

OTAN. (2022). *NATO 2022 Strategic Concept*. Retirado de https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

OTAN. (2024). Emerging and disruptive technologies [Página *online*]. Retirado de https://www.nato.int/cps/en/natohq/topics_184303.htm.

Ovum. (2018). *How to Achieve AI Maturity and Why It Matters: An AI maturity assessment model and road map for CSPs*. Retirado de https://www.amdocs.com /sites/default/files/filefield_paths/ai-maturity-model-whitepaper.pdf

Parlamento Europeu. (2024). *The EU AI Act - Article 3: Definitions*. Retirado de https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_EN.pdf

Portugal Digital. (2022). Estratégia Nacional de Dados [Página *online*]. Retirado de https://portugaldigital.gov.pt/acelerar-a-transicao-digital-em-portugal/conhecer-as-estrategias-para-a-transicao-digital/estrategia-nacional-de-dados/

Portugal INCoDe.2030. (2019). *AI PORTUGAL 2030: An innovation and grouth strategy to foster Artificial Intelligence in Portugal in the European context*. Retirado de https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3d%3dBAAAAB%2bLCAAAAAAABACzMDQxAQC3h%2byrBAAAAA%3d%3d

RAND Corporation. (2019). *The Department of Defense Posture for Artificial Intelligence*. Retirado de https://www.rand.org/pubs/research_reports/RR4229.html

Raska, M., & Bitzinger, R. A. (2023). *The AI Wave in Defense Innovation: Assessing Military Artificial Intelligence Strategies. Capabilities, and Trajectories*. New York: Routledge.

Recuperar Portugal. (s.d.). Plano de Recuperação e Resiliência [Página *online*]. Retirado de https://recuperarportugal.gov.pt/

Resolução do Conselho de Ministros n.º 131/2021, de 10 de setembro (2021). *Aprova a Estratégia para a Transformação Digital da Administração Pública 2021-2026 e o respetivo Plano de Ação Transversal para a legislatura*. Diário da República, 1.ª Série, 177, 17-34. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 30/2020, de 21 de abril (2020). *Aprova o Plano de Ação para a Transição Digital*. Diário da República, 1.ª Série, 78, 6-32. Lisboa: Presidência do Conselho de Ministros.

Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho (2019). *Aprova a Estratégia Nacional de Segurança do Ciberespaço 2019-2023*. Diário da República, 1.ª Série, 108, 2888-2895. Lisboa: Presidência do Conselho de Ministros.

Resolución 11197/2023, de 29 de junio, de la Secretaria de Estado de Defensa (2023). *Estrategia de desarrollo, implantación y uso de la Inteligencia Artificial en*

el Ministerio de Defensa. *Boletín Oficial del Ministerio de Defensa,* (131), pp. 19131-19140. Retirado de https://publicaciones.defensa.gob.es/media/ downloadable/files/ links/2/0/20230706.pdf

Ribeiro, A. S. (2009). *Teoria geral da estratégia: o essencial ao processo estratégico*. Coimbra: Almedina.

Ribeiro, A. S., & Pinto, S. S. (2022). *O Processo de Gestão Estratégica no Estado-Maior-General das Forças Armadas*. Lisboa: Instituto Universitário Militar.

Sadiq, R. B., Safie, N., Rahman, A. H. A., & Goudarzi, S. (2021). *Artificial intelligence maturity model: a systematic literature review*. Retirado de https://peerj.com/ articles/cs-661/#

Santos, L. A. B., & Lima, J. M. M. (.). (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação (2.ª ed, revista e atualizada). Cadernos do IUM, 8*. Lisboa: Instituto Universitário Militar.

Select Commitee On Artificial Intelligence. (2023). *National Artificial Intelligence Research and Development Strategic Plan: 2023 Update*. National Science and Technology Council. Washington, DC: Executive Office of the President of the United States. Retirado de https://www.whitehouse.gov/wp-content/uploads/2023/05/ National-Artificial-Intelligence-Research-and-Development-Strategic-Plan-2023-Update.pdf

Springer. (2023). *Artificial Intelligence: Definition and Background* [Página *online*]. Retirado de https://link.springer.com/chapter/10.1007/978-3-031-21448-6_2#Sec1

Tortoise. (2023). The Global Artificial Intelligence Index [Página *online*]. Retirado de https://www.tortoisemedia.com/2023/06/28/the-global-artificial-intelligence-index/

Vitrine AI Québec. (2022). *Artificial Intelligence Maturity Framework and Assessment Tool*. Retirado de https://api.vitrine.ia.quebec/storage/1434/vitrineia-rapportmaturite-en-vf.pdf

ESTUDO 2 – APLICAÇÃO DAS TECNOLOGIAS DE INTELIGÊNCIA ARTIFICIAL EM OPERAÇÕES MILITARES[1]

APPLICATION OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN MILITARY OPERATIONS

Rui Jorge Fernandes Bettencourt
Coronel TM

José Manuel dos Santos Coelho
Capitão-de-mar-e-guerra EMQ

RESUMO

A liderança do conhecimento e definição de tendências de evolução para as tecnologias de Inteligência Artificial concentra-se, fundamentalmente, na sociedade civil. A forte convergência das comunidades big data, poder computacional e investigação em algoritmos de *machine learning,* e as dinâmicas daí resultantes, representam um desafio respeitante à Segurança e Defesa. Esta investigação teve, assim, como objetivo propor contributos para melhorar a exploração das tecnologias de IA em operações militares pelas Forças Armadas (FFAA) portuguesas, pautando-se, metodologicamente, por um raciocínio indutivo, uma estratégia qualitativa e um desenho de pesquisa tipo estudo de caso, e associadamente, nas análises documental e de conteúdo das entrevistas a 22 entidades do Ministério da Defesa Nacional (MDN), das FFAA e do meio académico e empresarial. Dos resultados, conclui-se que: o MDN e as FFAA estão envolvidos em projetos no âmbito da IA; a Base Tecnológica e Industrial de Defesa possui competências e experiência no desenvolvimento de soluções e respetiva incorporação tecnológica em IA; existe capacidade técnica nacional para que os processos/sistemas identificados como prioritários alcancem níveis de maturidade *Technology Readiness Level* superior a sete até ao final da década. Neste seguimento, foram elencadas 17 propostas de melhoria da supradita exploração de tecnologias de IA pelas FFAA.

Palavras-chave: Inteligência Artificial, Operações Militares

[1] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Promoção a Oficial General (CPOG 2021-2022). A versão integral encontra-se disponível nos Repositórios Científicos de Acesso Aberto de Portugal (https://www.rcaap.pt/).

ABSTRACT

Knowledge leadership and the definition of evolution trends for Artificial Intelligence (AI) technologies are fundamentally focused on civil society. The strong convergence of communities in big data, computational power and research in machine learning algorithms, and the resulting dynamics, represent a challenge regarding Security and Defence. Thus, this investigation aimed to propose contributions to improve the capability of the Portuguese Armed Forces (FFAA) in the exploitation of AI technologies in military operations, methodologically guided by inductive reasoning, a qualitative strategy and a case study research design, and in the documental and content analysis of the interviews with 22 entities of the Ministry of National Defence (MDN), the FFAA and the academic and business sectors. From the results, it can be concluded that: the MDN and the FFAA are involved in projects within the scope of AI; the Defence Technological and Industrial Base partakes skills and experience regarding the development of AI solutions and respective technological incorporation in AI; there is national technical capacity for the processes/systems identified as priorities to reach maturity levels of Technology Readiness Level above seven by the end of the decade. In this follow-up, 17 proposals to improve the aforementioned capability of the FFAA were listed.

***Keywords**: Artificial Intelligence, Military Operations*

1. INTRODUÇÃO

O ambiente global de Segurança e Defesa está a ser transformado pela Inteligência Artificial (IA ou AI[2]), conforme reconhecem os países que integram a Organização do Tratado do Atlântico Norte (OTAN), assumindo a Aliança que estas tecnologias possuem um caráter estruturante (*foundational*) que irá provavelmente afetar todo o espectro das suas atividades (North Atlantic Treaty Organization [NATO], 2021b), num ambiente geopolítico extremamente competitivo, designadamente com a China que, do ponto de vista militar, encara as tecnologias de IA como uma oportunidade para saltar fases do processo de desenvolvimento de armamento e, assim, ultrapassar o *gap* que tem presentemente face aos Estados Unidos da América (Kanaan, 2020, p. 192).

Com uma aplicação transversal aos diferentes domínios operacionais, salienta-se o facto de serem já hoje algoritmos de aprendizagem (*learning algorithms*)

[2] Será igualmente utilizada a designação e abreviatura inglesa (AI – *Artificial Intelligence*) sempre que se utilizarem termos em que se considera adequado manter a designação inglesa (e.g. weak AI).

que guarnecem "postos de vigilância" das nações no ciberespaço (Domingos, 2015, p. 19), e que a utilização generalizada da IA será uma realidade e, face à tendência de evolução da IA autónoma enquanto produto tecnológico aplicado aos conflitos, conduzirá ao aumento do potencial de combate das Unidades (Parcelas, 2019).

Num período em que os recursos humanos (RH) nas Forças Armadas (FFAA) são limitados, designadamente em função da crescente complexidade dos sistemas de armas e da necessidade de assegurar em permanência a sua sustentação e condições de operacionalidade, e considerando igualmente a sua implicação na necessidade de redução da pegada humana projetada em Teatro de Operações, a aplicação de tecnologias de IA constitui-se como um real fator multiplicador de força (Costa, 2020).

Com papel crescente no campo de batalha, onde algoritmos de aprendizagem pesquisam sobre imagens de reconhecimento, processam *after action reports*, e atualizam a imagem situacional para o comandante, a aplicação de algoritmos de *machine learning*[3] (ML) permite olhar o futuro, em analogia à introdução do radar na Batalha de Inglaterra, possibilitando que não se reaja apenas às ações do adversário, mas que se consiga prever os seus movimentos e atuar em antecipação (Domingos, 2015, p. 19).

Neste âmbito, e face à forma como os sistemas de armas robóticos estão a influenciar já hoje o espaço de batalha, Paul Sharre (2018, p. 364) salienta que "o futuro está a chegar, e não estamos prontos". O momento atual, "com uma forte convergência de três comunidades, *big data*, poder computacional e investigação em algoritmos de ML, assim como a menos visível influência do valor financeiro associado para gerar rendimento" (Kepner & Gadepally, 2020), em que a liderança do

---

[3] ***Machine Learning*** **(ML)** – Para a ciência de dados (*data science*), o conceito básico de *machine learning* envolve a utilização de métodos estatísticos de aprendizagem e otimização que permitem que os computadores analisem conjuntos de dados e identifiquem padrões. As técnicas de *machine learning* potenciam a pesquisa de dados (*data mining*) para identificar tendências históricas para extrapolação em modelos futuros. Genericamente, um algoritmo típico de *supervised machine learning* é composto por três componentes: 1. Um processo de decisão, envolvendo um conjunto de cálculos ou outras etapas em que processa os dados de entrada e devolve uma "suposição" (*guess*) sobre o tipo de padrão nesses dados, que o seu algoritmo procura encontrar uma função de erro, consistindo num método para medir a qualidade da "suposição", comparando-a com exemplos conhecidos (quando disponíveis). 3. Um processo de atualização ou otimização, onde o algoritmo analisa o erro e, em seguida, atualiza a forma como o processo de decisão alcança a decisão final, para que na próxima oportunidade o erro seja menor. Muitos modelos de *machine learning* são definidos em função da presença, ou ausência, da influência humana sobre os dados em bruto, seja na atribuição de recompensa, num feedback específico, ou utilização de "rótulos" (labels), considerando-se existir os seguintes tipos de ML: s*upervised learning; unsupervised learning, semisupervised learning, reinforcement learning, e deep learning* [descritos neste Apêndice] (Tamir M., 2020).

conhecimento e definição de tendências de evolução para tecnologias emergentes e disruptivas como a IA se concentra essencialmente na sociedade civil (NATO, 2021b), assente numa dinâmica de evolução tecnológica tal que, "pela primeira vez, se está perante a possibilidade real de outras entidades - entidades criadas por nós – poderem vir a tornar-se inteligentes" (Oliveira, 2017, p. 7), representa igualmente um enorme desafio em termos de Segurança e Defesa, realidade previamente ecoada pelo professor Pedro Domingos (2015, p. 285):

> O nosso trabalho no mundo das máquinas inteligentes será assegurar que fazem o que pretendemos, tanto nos dados de entrada (definindo os objetivos) como no resultado (verificando que se obteve o que se pediu). Se não o fizermos, alguém o fará. As máquinas podem ajudar-nos a identificar coletivamente o que pretendemos, mas se não participarmos, perdemos mais do que ganhamos.

Neste enquadramento o principal objetivo da presente investigação é propor contributos para melhorar a exploração das tecnologias de IA em operações militares pelas FFAA portuguesas. Para o atingir são objetivos específicos (OE): OE1: Analisar a aplicação da IA no meio civil; OE2: Analisar a aplicação da IA nas OpMil realizadas pelas FFAA portuguesas. Um conjunto de objetivos plasmados na questão central (QC) orientadora do trabalho: Como melhorar a capacidade de exploração das tecnologias de IA em OpMil pelas FFAA portuguesas?

Em termos de estrutura, este documento é constituído por sete capítulos, sendo o atual a introdução. O segundo, destina-se à revisão da literatura e apresentação do modelo de análise adotado na investigação. O terceiro, à descrição da metodologia seguida e do método, descrevendo-se os participantes e procedimento seguido, assim como os instrumentos de recolha de dados e as técnicas utilizadas no seu tratamento. No quarto, quinto e sexto capítulos efetuou-se a análise dos dados e resposta às questões de investigação. O sétimo, e último, norteado pelas conclusões, apresentam-se os contributos para o conhecimento, limitações e propostas de estudos futuros.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

Apresenta-se no presente capítulo a informação decorrente do processo de revisão da literatura, à luz dos dois conceitos estruturantes – IA e OpMil –, assim como o modelo de análise.

2.1. Inteligência Artificial

IA é um conceito com referências que remontam a 1950, ocorrendo a primeira utilização da sua atual designação em 1955, através do professor John McCarthy (Moor, 2006), na proposta que efetuou para a realização do evento "*The Dartmouth Summer Research Project on Artificial Intelligence*" (McCarthy, Minsky, Rochester, & Shannon, 1955).

A abrangência que envolve, com muitas técnicas e teorias desenvolvidas ao longo dos anos (Oliveira, 2017, p. 86) – muito potenciado pelos significativos avanços verificados nos últimos dez a 15 anos (Kanaan, 2020, p. xviii) –, proporciona o contacto com um conjunto alargado de conceitos e definições, não existindo uma definição consensual. Não obstante "[...] o termo 'inteligência artificial' [ter] entrado na linguagem comum e se tenha tornado trivial nos *media* [...]" (Conselho Europeu, 2021), o facto é que o alcance e impacto destas tecnologias se encontra sintetizado na analogia de Andrew Ng (2017), que descreveu a IA como algo tão transformador para a sociedade como o foi a introdução da eletricidade.

Neste enquadramento, adotou-se a definição plasmada na iniciativa que enforma a estratégia nacional para a IA (Iniciativa Integrada de Política Pública Dedicada ao Reforço de Competências Digitais [INCoDe.2030], 2021), como "a área científica e o conjunto de tecnologias que utilizam programas e dispositivos físicos para imitar facetas avançadas da inteligência humana".

As tecnologias de IA têm o objetivo de criação de sistemas de computadores capazes de aprender e melhorar o seu desempenho, à medida que adquirem mais dados e experiência relacionados com as tarefas que lhes foram atribuídas (Kanaan, 2020, p. 118), atuando estes sistemas:

> […] na esfera física ou digital reunindo dados, por meio de sensores, câmaras ou outros recetores, interpretando-os e processando a informação deles derivada, para perceção do ambiente e decisão da melhor ação face ao objetivo inicialmente definido. […] As ações podem ser executadas digitalmente, quando integradas num sistema de tecnologias de informação, ou serem uma solução física, como ocorre em robótica. (Agência para a Modernização Administrativa [AMA], 2021, p. 11)

Recorre-se ainda à estratégia nacional para salientar que:

> Os mecanismos de IA podem apresentar ferramentas como (mas não necessariamente limitadas): Autonomia, resolução de problemas, planeamento complexo, negociação, raciocínio, inferência, tomada de decisão, diagnóstico, previsão, aprendizagem com a experiência, adaptação a novas situações, compreensão e geração de linguagem, explicação, argumentação, reconhecimento visual/áudio e de objetos. (INCoDe.2030, 2021)

Considera-se na IA a abstração conceptual de duas áreas, a *narrow AI* e a *general AI*, onde a primeira enquadra a teoria e o desenvolvimento de sistemas computacionais que executam tarefas que incrementam (*augment*) a inteligência humana, designadamente perceber (*perceiving*), classificar, aprender, abstrair, raciocinar e/ou agir (*acting*), enquanto a segunda se refere à autonomia total (*full autonomy*) (Kepner & Gadepally, 2020).

Esta conceptualização assume diferentes designações, sendo frequente as referências para os mesmos âmbitos em torno, respetivamente, de *weak AI* e *strong AI*, como no caso alemão, onde a estratégia do Governo Federal para a IA e, por consequência, o conceito de IA do Exército da Alemanha (ExA) (2019, p. 28), se concentra na *"weak (or narrow) AI"*.

Ao nível de Portugal, existe projeção externa sobre o trabalho em curso, onde o *Global AI Index* (Tortoise, s.d.), modelo de caracterização e comparação entre 62 países quanto à adoção de tecnologias de IA, apresenta Portugal na 35.ª posição (Quadro 1).

Quadro 1 – Extrato do Global *AI Index* (valores de ordenação relativa por dimensão)

País	Dimensões								
	Talentos	Infraestruturas	Ambiente Operacional	Investigação	Desenvolvimento	Estratégia Governamental	Comércio		
								Ordem	Pontos
Estados Unidos da América	1	4	35	1	1	17	1	1	100
China	24	1	6	2	2	2	2	2	62,90
(…)									
Alemanha	11	13	30	6	12	10	8	9	36,04
França	9	14	17	16	15	5	10	10	34,42
(…)									
Espanha	21	19	23	26	29	4	28	21	26,95
(…)									
Portugal	32	36	16	38	40	22	35	35	20,89
(…)									

Outro indicador, orientado para as dimensões de *Research and Development* (R&D) e de *Economy*, o índice *Global AI Vibrancy Tool: Who's leading the global AI race?* (Stanford Institute for Human-Centered Artificial Intelligence [HAI], s. d.) permite analisar as evoluções anuais para destas dimensões entre 2017 e 2020 (Figura 1).

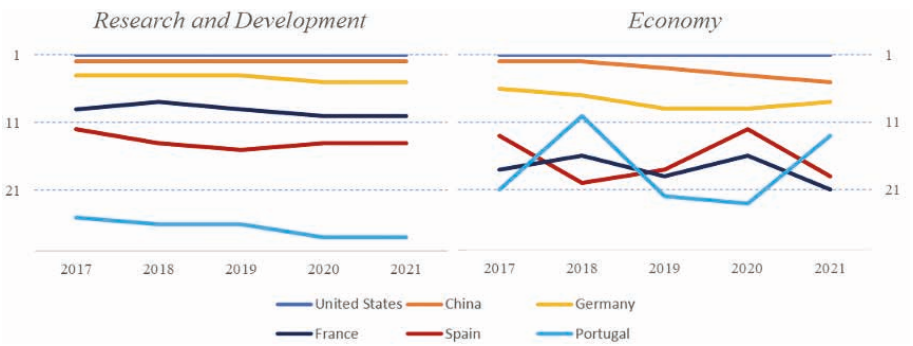

Figura 1 – HAI AI Index (adaptação com posições relativas de países)
Fonte: Adaptado a partir de HAI (s.d.).

Portugal encontra-se atualmente na 35.ª posição (em 62 países) no *Global AI Index* e na 20.ª posição (em 29 países) do *HAI AI Index*, neste último, posicionado na 28.ª posição de R&D e na 13.ª posição na dimensão de economia, onde se verifica algum dinamismo ao nível de submissão e atribuição de patentes (Figura 2), assim como no investimento privado em IA e criação de novas empresas (Figura 3) (HAI, s.d.).

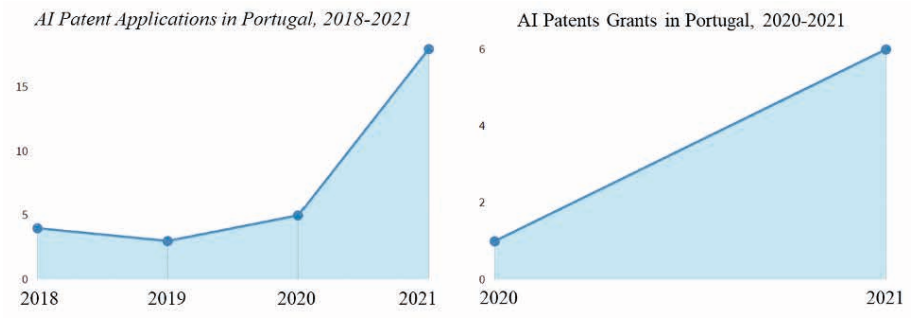

Figura 2 – HAI AI Index (exemplo de indicadores R&D de Portugal)
Fonte: Adaptado a partir de HAI (s.d.).

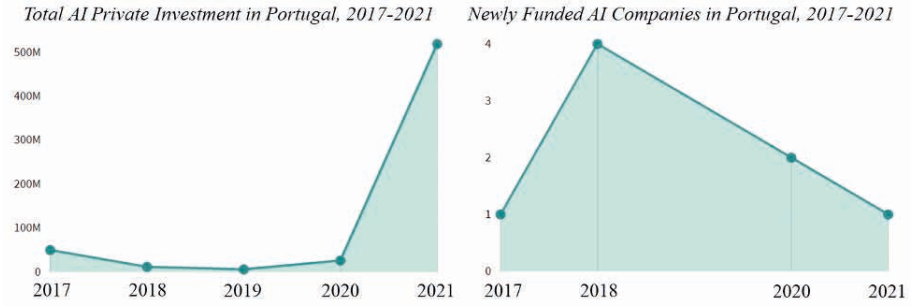

Figura 3 – HAI AI Index (exemplo de indicadores económicos de Portugal)
Fonte: Adaptado a partir de HAI (s.d.), investimentos em *start-ups AI* em dólar americano.

Não foi identificada fonte nacional equivalente, existindo, contudo, dados de indicadores no âmbito do Observatório das Competências Digitais (INCoDe.2030, 2020).

No âmbito da administração pública portuguesa, um estudo realizado em 2020 pela *Microsoft* e pela *Ernst & Young Global Limited*, reconheceu que a maioria das entidades do setor público têm limitadas estruturas de IA, identificando o setor da saúde como tendo a maior taxa de implementação de IA (AMA, 2021, p. 30).

A estratégia nacional para a IA (INCoDe.2030, 2019) identificou várias ações [linhas de ação (LA)], salientando-se as de maior relevância para a presente investigação:

- Áreas de especialização em Portugal com impacto internacional
  […] Processamento de linguagem natural; tomada de decisão em tempo real com IA; IA para desenvolvimento de *software*; e IA para computação de ponta [*edge-computing*].
- Áreas de pesquisa e inovação em redes europeias e internacionais
  […] Transformação urbana através de cidades sustentáveis; Sistemas de energia sustentáveis; Meio ambiente e biodiversidade: das florestas e da economia verde às espécies marinhas e da economia azul; Mobilidade e condução autónoma; CiberSegurança; Saúde; e Indústria.
- Pesquisa fundamental para a IA do Futuro
  […] IA transparente [*explainable AI*], dando aos algoritmos a capacidade de explicar as suas próprias decisões e fornecer um relato de alto nível e adaptável para promover a equidade e a responsabilização; IA emocional: os algoritmos utilizarão emoções para alcançar melhores decisões; IA autónoma: importante não só no setor automóvel, mas também em sistemas de informação, cibersegurança, cidades inteligentes, indústria, etc.; AutoML: sistemas inteligentes que podem usar a aprendizagem da máquina [*machine learning*] de forma autónoma; Criatividade Computacional: a produção e criação de produções artísticas estão hoje em dia confinadas principalmente à ação humana. […].

Assinala-se a ausência de referência à Defesa Nacional na estratégia nacional, particularmente quando em comparação com as referências explícitas na francesa "*our task force recommends avoiding spreading efforts too thinly, but rather focus on four key sectors: healthcare, environment, transportmobility and defense-security*" (Villani, 2018, p. 3), na alemã, "*The use of AI-based technologies and systems will have implications for the armed forces and is therefore an important issue to be taken into account for the future of the Bundeswehr*" (Governo Federal da Alemanha, 2018, p. 31), assim como na espanhola, salientando a Estratégia de Tecnologia e Inovação para a Defesa, no âmbito das iniciativas de promoção da IA na atividade económica e empresarial (Governo de Espanha, 2020, p. 52), tendo o

Ministério da Defesa de Espanha integrado o grupo de trabalho interministerial que desenvolveu a estratégia de IA do Governo de Espanha (2020, p. 88).

2.2. Operações militares

A operacionalização deste conceito em termos da aplicação de tecnologias de IA está subjacente ao preconizado no Conceito Estratégico Militar (Conselho de Chefes de Estado-Maior [CCEM], 2014a, pp. 26-28), no âmbito da caracterização do conceito de ação militar, como a "referência essencial para o desenvolvimento das estratégias operacional, genética e estrutural", o qual:

> Caracteriza a atuação das Forças Armadas, ao nível estratégico-militar, nos empenhamentos em tempo de paz, exceção/crise e guerra, respeitando os cenários identificados. […] o que determina que se disponha, em permanência, e com aptidão para operar em todo o espectro de operações militares, de estruturas de Comando e Controlo (C2) e de ciberdefesa; estruturas de informações até ao nível estratégico militar; forças de operações especiais; forças e unidades navais com valências para a guerra de superfície, antiaérea, antissubmarina, submarina e anfíbia; forças terrestres ligeiras, médias e pesadas […] através de um amplo leque de tipologia de forças, como também, a possibilidade de mobilizar pessoal e reativar meios e unidades militares; forças e unidades aéreas com valências em luta aérea defensiva e ofensiva, operações aéreas de apoio, vigilância e reconhecimento e contribuição para operações terrestres e marítimas.

Na doutrina de referência OTAN, retira-se "operação" como a sequência coordenada de ações com um propósito definido, podendo esta contribuir para uma aceção mais alargada, que incluí as ações não-militares, sendo explicitado que se encontra subjacente a natureza militar (North Atlantic Treaty Organization Standardization Office [NSO], 2020, p .94).

Considera-se relevante evidenciar o entendimento para ambiente operacional (*operating environment*), referente ao conjunto de condições, circunstâncias e influências que afetam o emprego de capacidades militares e têm impacto nas decisões de um comandante (NSO, 2020, p. 94), assim como salientar que se encontra subjacente ao âmbito da investigação a capacidade de *reach back*,

definida como o processo de fornecimento às forças destacadas de serviços e capacidades de especialistas externos ao Teatro de Operações (NSO, 2020, p. 107).

Para fins do presente estudo, considera-se Operação Militar como a sequência coordenada de ações com propósito definido, empreendidas para o cumprimento de missões das FFAA, num determinado ambiente operacional. Para as FFAA portuguesas, as missões são especificadas no documento "Missões das Forças Armadas" (CCEM, 2014b), tendo em atenção os diversos cenários levantados e os Objetivos Estratégicos Militares definidos, decorrendo as mesmas da Constituição da República Portuguesa e da lei (CCEM, 2014a, p. 37). Para auxiliar o comandante a integrar, sincronizar e dirigir as diferentes capacidades e atividades colocadas à sua disposição numa operação, foi desenvolvido e introduzido na doutrina da OTAN o conceito de funções de combate, consistindo num "grupo de tarefas e sistemas (pessoas, organizações, informação e processos) unidos por uma finalidade comum que os comandantes aplicam para cumprir missões operacionais e de treino" (Estado-Maior do Exército, 2012, p. 37).

Assumem especial relevância para a investigação as funções de combate comuns a todos os níveis das operações conjuntas (*joint functions*): manobra, fogos, C2, informações (*intelligence*), atividades de informação e influência[4] (*information*), apoio logístico (*sustainment*), proteção da força e cooperação civil-militar (CIMIC) (NSO, 2019, pp. 1-21-1-27).

No documento "*AI and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment*" (Cooperative Cyber Defence Centre of Excellence [CCDCOE], 2021, pp.13-14), é salientado que a estratégia para a IA da OTAN refere a necessidade de os seus membros trabalharem para integrar a IA de forma interoperável nos sistemas militares, enfatizando a importância da cooperação entre a OTAN, o setor privado e a academia, no desenvolvimento de IA para fins de defesa.

São consideradas no referido documento como áreas de potencial impacto da IA na melhoria das forças militares: C2, comunicações, computadores, informações, vigilância e reconhecimento (C4ISR); armamento e efeitos; veículos autónomos; planeamento de capacidades; nuclear, biológico, químico e radiológico (NBQR); medicina; gestão empresarial; logística; ciberespaço (*Cyber and Information Space*);

[4] Doravante referida por atividades de informação.

e treino (North Atlantic Treaty Organization Science & Technology Organization [STO], 2019, pp. 55-56).

A agenda NATO 2030 apresentou a ambição da OTAN com vista a garantir que se mantem pronta, forte e unida para enfrentar uma nova era de crescente competitividade global (NATO, 2021a), e onde os ministros dos negócios estrangeiros acordaram na *Charter of the Defence Innovation Accelerator for the North Atlantic* (DIANA) (NATO, 2022b), materializada em dois gabinetes regionais, 47 centros de teste e nove sites aceleradores de inovação (Missão Permanente de Portugal junto da Organização do Tratado do Atlântico Norte [DELNATO], 2022a; DELNATO, 2022b; NATO, 2022a). Neste âmbito, foram aceites as propostas nacionais (DELNATO, 2022a) para constituir o Centro de Experimentação Operacional da Marinha como centro de teste para as áreas da IA, Autonomia, Dados e Materiais, assim como o Arsenal do Alfeite como site acelerador de inovação (M. F. Pinto, mensagem de correio eletrónico [E-mail], 14 de abril de 2022).

Da revisão de literatura efetuada, referente à postura face às tecnologias de IA de FFAA de países da OTAN e União Europeia (UE), foi possível obter e analisar documentação referente a França, Alemanha e Espanha, países com maior investimento em IA na UE (Comissão Europeia, s.d.).

2.3. Outras FFAA e as tecnologias de IA

2.3.1. França

O relatório referente à utilização de IA em apoio da Defesa, do Ministério da Defesa de França [MDNFra] (2019, p. 9), estabelece linhas orientadoras para aplicação controlada de IA na Defesa, em torno da manutenção de liberdade de ação e interoperabilidade com os aliados, a garantia de IA confiável, controlável e responsável, a preservação da resiliência e capacidade de atualização dos sistemas, e na necessidade de manter o seu "*sovereign core*", estabelecendo um *roadmap*, sintetizando da seguinte forma as áreas de prioridade:

> *AI will help to filter, enhance, exploit and share data and provide help with manoeuvres, and hence offer combatants informed choices so that they can take decisions more quickly while reducing uncertainty (humans still take the decisions). Human-machine interactions will benefit from the contribution of AI, partly through augmented human-machine interfaces and partly through optimised cooperation*

between units, systems and combatants (including human/robot cooperation). (MDNFra, 2019, p. 15)

As áreas prioritárias de aplicação são as que se apresentam no Quadro 2.

Quadro 2 – Áreas prioritárias para aplicação de IA para Ministério da Defesa de França

Áreas de foco	Aplicação
Apoio à decisão e ao planeamento	– Sistemas para a condução de operações a nível estratégico e para o planeamento, especialmente logístico (com manutenção preditiva)
Combate colaborativo	– Fusão de dados de consciencialização situacional (aliados e inimigos) – Ajuda à mobilidade e à reação militar – Afetação automática de alvos entre vários efectores
Cibersegurança e influência digital	– Deteção de tentativas de ciberataque – Análise dos pontos fracos – Análise e antecipação de ameaças – Assistência a operações cibernéticas (defesa e ataque)
Logística e prontidão operacional	– Desempenho da missão e aplicações de manutenção assistida, especialmente para a cooperação com países que têm os mesmos sistemas que nós
Intelligence	– Automatização da exploração de grandes volumes de dados – Fusão de dados de várias fontes – Deteção de sinais fracos – Extração e resumo de dados
Robótica e autonomia	– Módulos de comportamento robótico evoluído (excluindo robôs de combate e drones e os que transportam sensores especializados altamente sensíveis)
IA nos serviços de apoio	– Apoio à decisão e análise preditiva a fim de programar, simular ou otimizar o consumo de recursos – Automatização de tarefas repetitivas e morosas, utilizando robôs de software para processos de fluxo transacional – Agentes ou utilizadores aumentados, utilizando chatbots

Fonte: Adaptado a partir de MDNFra (2019, pp. 15-19).

2.3.2. Alemanha

Da análise do *position paper "Artificial Intelligence in Land Forces"*, desenvolvido pelo Centro de Desenvolvimento de Conceitos e Capacidades do ExA (2019, p. 12), é possível extrair aplicações para a IA em todos os domínios de capacidade, armas e serviços em forças terrestres, categorizando-as por LA, com base na *NATO Comprehensive Operations Planning Directive*.

No documento são traçadas as LA no âmbito da organização e infraestruturas, designadamente, o recrutamento de especialistas de IA, a cooperação entre militares, a investigação e industria; a cooperação internacional; a utilização de estruturas de teste e experimentação; e organização e infraestrutura de dados IA,

salientando-se as recomendações inseridas nesta área para a criação uma "*National Defence Agency*" e, no Ramo, uma entidade coordenadora central "*AI Work Bench*" e um "*AI Development Centre*" (ExA, 2019, pp. 14-19), apresentando-se no Quadro 3 as LA por áreas de aplicação.

Tabela 1 – Áreas de aplicação da IA e linhas de ação do Exército da Alemanha

Áreas	LA
Análise de imagem	Referência de processamento de imagem
	Reconhecimento e identificação de alvos
Sistema aéreo tático não tripulado (TaUAS)	Reconhecimento
	Barreiras
	Efeitos
	Quadro jurídico
Sistema de Gestão de Combate de Nova Geração (NGBMS)	Referência do processo de tomada de decisão
	Controlo do fogo com base na IA
	Gestão da informação de IA
	NGBMS
	Aceleração do processo de decisão
Material e infra-estruturas	Iniciativa: Análise de erros baseada em IA
	Iniciativa: Configuração baseada em IA
Métodos de análise	Reconhecimento baseado em IA/*big-data*
	Análise diferencial de cenas por IA

Fonte: Adaptado a partir de ExA (2019, pp. 22-26).

2.3.3. Espanha

O documento "*La Fuerza 35*" apresenta a visão do Comandante do Exército de Espanha, assumindo que a constante evolução dos riscos e ameaças no ambiente operacional exigem uma constante adaptação, a materializar na *La Fuerza 35* (Exército de Espanha [ExEsp], 2019, p. 2), sendo a IA considerada como uma das principais tecnologias influenciadoras deste ambiente (ExEsp, 2019, p. 10), apresentando-se na Figura 4 a evolução planeada.

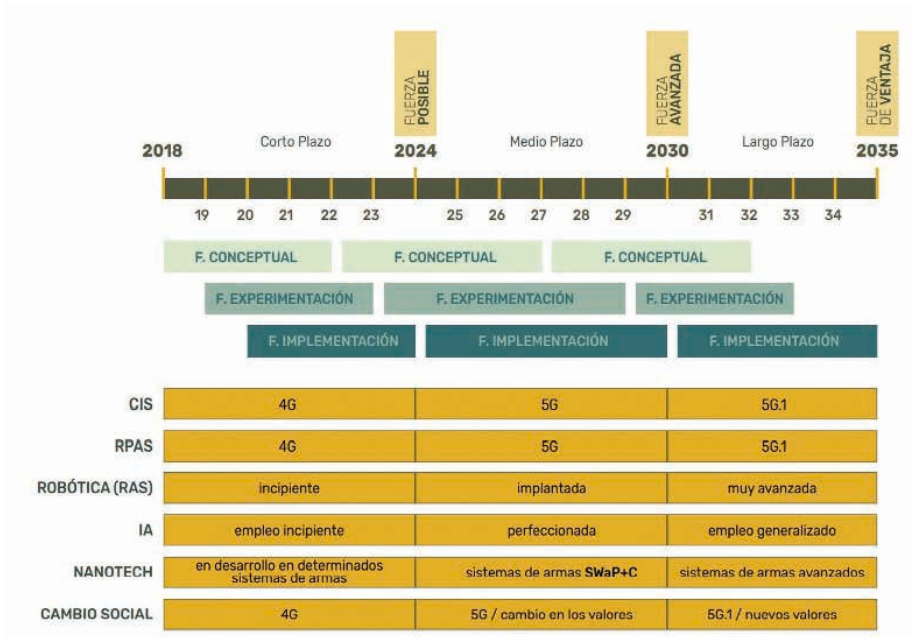

Figura 4 – Distribuição da evolução da transformação até 2035 (*Fuerza 35*)
Fonte: ExEsp (2019, p. 20).

Na Tabela 2 apresenta-se, por funções de combate, a evolução em termos de incorporação de tecnologias de IA ao serviço da *Fuerza 35*, assim como, na Figura 5, um pictograma síntese dos estádios previstos dessa evolução e prioridades identificadas.

Tabela 2 – Evolução planeada de incorporação de tecnologias de IA na *Fuerza 35*

Funções de Combate	Evolução
C2	Até 2030: Mobilidade de Posto de Comando: Sistema de apoio à tomada de decisão com IA; Guerra Eletrónica: Sistemas autónomos de *jamming* baseados em algoritmos de IA. Até 2035: Ciberdefesa: Emprego da IA para ação de supressão de defesas e ação ofensiva (*acción strike*).
Informações	Até 2030: Incremento do conhecimento situacional: Sistemas suportados em IA para recolha, avaliação e fusão de informação e distribuição de forma autónoma. Até 2035: Reconhecimento e Vigilância Terrestre: *Nano Robots* autónomos com IA (subsolo, grutas, etc.)

[Cont.]

Fogos	A utilização de IA e híper conectividade com a utilização de *big data* irá melhorar a gestão e eficácia das ações, com a introdução do conceito de "fogos em rede", permitindo a fusão de informação dos sensores próprios com a obtida através de sensores externos, como satélites.
Logística	A logística será baseada no conhecimento situacional e na antecipação da procura, no envio direto e na gestão do fluxo de recursos, onde as tecnologias de ponta permitirão agilizar e otimizar os processos, possibilitando uma redução significativa de pessoal e plataformas no Grupo Logístico em relação aos números atuais.
Proteção da Força	Até 2024: Consciência situacional: Criação de redes *mesh* com IA e realidade aumentada que garantam a sobrevivência do combatente.
Manobra	Resultará da integração da manobra no domínio físico com a manobra de informação, travada no domínio virtual e cognitivo, com as suas dimensões de ciberespaço, perceções e comportamento humano, com recursos próprios e adicionais, uma parte importante dos quais será disponibilizada em *reach back*.

Fonte: Adaptado a partir de ExEsp (2019, pp. 32-49).

2.4. Modelo de análise

A investigação efetuada considerou, para o conceito de IA, uma adaptação do estudo efetuado pelo Departamento de Defesa dos Estados Unidos da América (Tarraf et al., 2019), qualitativo, considerando e caracterizando as dimensões de análise da seguinte forma:

- Organização: a visão estratégica sobre a postura das instituições, composta pela visão, estratégia e alocação de recursos; as estruturas e unidades orgânicas para apoio dessa visão; e os *stakeholders* e seu mandato, autoridade e funções;
- Progresso: pesquisa, desenvolvimento e criação de protótipos e ferramentas para verificar, validar, testar e avaliar as tecnologias à medida que elas se desenvolvem e incrementam o seu nível de maturidade;
- Adoção: todos os aspetos referentes à aquisição, implementação, manutenção, e gestão do ciclo de vida das tecnologias, e adaptação doutrinária; conceitos de operações; técnicas, táticas e procedimentos (TTP); e parcerias ou outros processos para melhor retirar partido destas tecnologias;
- Inovação: a cultura interna de inovação e as várias opções e mecanismos para incorporar na instituição inovações externas ou elementos

particularmente inovadores.

– Dados: dimensão abrangente e específica da IA, assumindo dados como um recurso; as regras e políticas de governação que envolvem a sua obtenção e utilização; e a capacidade de armazenamento, de computação, de comunicações e de outras infraestruturas técnicas necessárias para potenciar o recurso a dados em escala (*data at scale*);
– Talentos: O capital humano necessário para desenvolver, adquirir, manter e operar as tecnologias de IA; e os mecanismos para recrutar, reter, cultivar e desenvolver talentos ao longo das suas carreiras.

Da análise das dimensões apresentadas, procurou extrair-se ainda observações para efeitos de elaboração de análise SWOT – *Strengths* (swS), *Weaknesses* (swW), *Opportunities* (swO), and *Threats* (swT), com vista à identificação dos contributos resultantes da investigação.

Para o conceito de OpMil, considerou-se como dimensões de análise as funções de combate comuns a todos os níveis das operações conjuntas, considerando como indicadores em cada uma das dimensões as áreas onde a IA terá maior impacto na melhoria das forças da OTAN (CCDCOE, 2021, p. 14) (Tabela 3).

Tabela 3 – Áreas onde a IA terá maior impacto na melhoria das forças da OTAN

Área	Descrição
C4ISR	– Veículos autónomos farão *Intelligence, Surveillance, and Reconnaissance,* obtendo grandes quantidades de dados e através do acesso a áreas demasiado perigosas para intervenção humana; – Os algoritmos de IA consolidarão e analisarão dados (ex.: detetar padrões de vida, mapeamento humano no terreno e análise de redes sociais) de várias fontes e sensores, e fornecerão apoio à decisão aos operadores humanos; – A IA será usada para reconhecimento de imagem e discriminação de alvos; – A IA melhorará os sistemas de alerta antecipada (*early warning*) e servirá como assistente virtual para os operadores humanos.
Armas e Efeitos	– *Cross-cueing* (cruzamento de diferentes fontes / sensores); – Planeamento de trajetórias; – Evitar colisões / *swarming*; – Seleção de armas; – Avaliação de danos (de batalha); – Coordenação de efeitos.
Veículos Autónomos	– Planeamento de trajetórias; – Evitar colisões / *swarming*; – Apoio ao operador (ex.: um operador a controlar vários veículos não tripulados); – Planeamento dinâmico para sistemas autónomos (ex.: navegação, obtenção de dados, caracterização da situação e sensores adaptativos); – A ia permitirá "sistemas autónomos contra engenhos explosivos improvisados em áreas urbanas" e "veículos submarinos não tripulados de longa duração".

[Cont.]

Planeamento de Capacidades	– Apoio à tomada de decisão complexa que cruza os limites internos tradicionais; – Apresentação de avaliações de fatores complexos e de efeitos em cadeia aos decisores.
NBQR	– melhorar a deteção, identificação e monitorização rápida de ameaças NBQR por meio de posicionamento e integração de sensores, e da fusão e interpretação de dados.
Apoio Sanitário	– Desenvolver conhecimento clínico baseado em evidências, diagnóstico baseado em evidências e melhores práticas de tratamento para reduzir a morbidade e mortalidade e manter/recuperar funções essenciais perante os perigos resultantes da missão; – Fornecer apoio à decisão automatizado e ferramentas de apoio de diagnóstico para auxiliar os médicos no terreno que se encontram perante novas situações de trauma.
Apoio à Decisão e Gestão	– Análise avançada [*data analytics*] e tomada de decisão baseada em evidências; – Apoio na análise de custos, avaliação de impacto económico e tendências (*drivers*); – Apoio à decisão baseado em evidências em tempo útil.
Logística	– Minimizar o tempo de inatividade do equipamento; – Minimizar falhas do sistema; – Melhorar a gestão da manutenção e de stocks, etc..
Ciberespaço e espaço informacional	– A IA desempenhará um papel na edificação de redes autónomas resilientes e na ciberguerra, avaliando e interpretando grandes quantidades de sensores e dados de informações e detetando, avaliando e respondendo ao ambiente onde atua.
	– Os sistemas de IA (especialmente em combinação com sistemas de realidade virtual/aumentada) têm o potencial de melhorar o treino individual e personalizado, através da capacidade de adaptação em tempo real ao comportamento humano e da capacidade de gerar ambientes ou cenários de treino personalizados.

Fonte: Adaptado a partir de CCDCOE (2021, pp. 14).

O modelo de análise encontra-se apresentado no Quadro 3.

Quadro 3 – Modelo de análise

<table>
<tr><td rowspan="2">OG</td><td colspan="4">Propor contributos para melhorar a exploração das tecnologias de IA em OpMil pelas FFAA portuguesas.</td></tr>
<tr><td>QC</td><td colspan="3">Como melhorar a capacidade de exploração das tecnologias de IA em OpMil pelas FFAA portuguesas?</td></tr>
<tr><td>Objetivos Específicos (OE)</td><td>Questões Derivadas (QD)</td><td>Conceitos Estruturantes</td><td>Dimensões</td><td>Indicadores</td></tr>
<tr><td rowspan="8">OE 1
Analisar a aplicação da IA no meio civil.</td><td rowspan="8">QD 1
Como é que a IA é aplicada no meio civil?</td><td rowspan="8">IA</td><td>Organização</td><td>– Visão, estratégia e alocação de recursos;
– Estruturas organizacionais no âmbito da inovação (em particular de IA).</td></tr>
<tr><td>Progresso</td><td>– Atividades e portfólio de investigação e desenvolvimento;
– Protótipos;
– Verificação, validação, teste e avaliação.</td></tr>
<tr><td>Adoção</td><td>– Aquisições;
– Tecnologias em operação;
– Desenvolvimento de doutrina, conceitos de emprego, TTP e processos.</td></tr>
<tr><td>Inovação</td><td>– Cultura de inovação;
– Mecanismos para tirar partido da inovação.</td></tr>
<tr><td rowspan="2">Dados</td><td>– Dados como recursos;</td></tr>
<tr><td>– Mecanismo de governação de coleções de dados e utilização;
– Armazenamento, computação, e outras infraestruturas</td></tr>
<tr><td>Talentos</td><td>– Talentos necessários para desenvolver, adquirir, sustentar e operar;
– Recrutamento e retenção.</td></tr>
<tr><td></td><td></td><td></td><td>[Mesmas da QD1]</td><td>[Mesmos da QD1]</td></tr>
</table>

[Cont.]

OE 2 Analisar a aplicação da IA em OpMil nas FFAA portuguesas.	**QD 2** Qual a aplicação da IA em OpMil nas FFAA portuguesas?	OpMil	Manobra Fogos C2 Informações Atividades de Informação e Influência Apoio Logístico Proteção da força CIMIC	– C4ISR – Armas e Efeitos – Veículos Autónomos – Planeamento de Capacidades – NBQR – Apoio Sanitário – Apoio à Decisão e Gestão – Logística – Ciberespaço e espaço informacional – Treino

3. METODOLOGIA E MÉTODO

Metodologicamente, este estudo assenta num raciocínio indutivo, associado a uma estratégia qualitativa (Santos & Lima, 2019), a fim de analisar formas como as FFAA poderão preparar-se para retirar o melhor partido de tecnologias emergentes e disruptivas, designadamente de IA. Tem como desenho de pesquisa o estudo de caso, procurando-se recolher dados sobre o potencial de aplicação das tecnologias de IA em OpMil nacionais (Santos & Lima, 2019), a fim de procurar avaliar a aplicabilidade da IA em OpMil, bem como prioridades e caminhos a percorrer para a sua concretização.

Integraram esta investigação 22 entidades, sendo 14 do Ministério da Defesa Nacional (MDN), Estado-Maior-General das Forças Armadas (EMGFA) e ramos, com responsabilidade direta nos processos em torno da inovação e das tecnologias emergentes e disruptivas, e oito fora do âmbito restrito das estruturas da Defesa Nacional, designadamente académicas e empresariais, relevantes para a estratégia nacional para a IA, cinco das quais indicadas pela *AED*[5] *Cluster Portugal*[6] (doravante designadas, respetivamente, de internas e externas). Este quantitativo, aplicado a um grupo com alguma excecionalidade, encontra-se enquadrado no intervalo N=6 a 10 definido por Rego, Cunha e Meyer (2018, p. 53).

[5] *Cluster* de indústrias nacionais na área da Aeronáutica, Espaço e Defesa.
[6] Com intenção de auscultar empresas da Base Tecnológica de Indústrias de Defesa, solicitou-se o apoio da Direção-Geral de Recursos de Defesa Nacional, fazendo a ligação com o *Cluster* AED.

Tabela 4 – Lista de entrevistados

Função	Entidade
Diretor da Direção de Comunicações e Sistemas de Informação (Exército)	Brigadeiro-general Paulo Fernando Viegas Nunes
Subdiretora-Geral da Polícia Judiciária	Dra. M. Luísa Proença
Chefe da Divisão de Planeamento de Forças do Estado-Maior do Exército	Coronel Tirocinado Luís Miguel Afonso Calmeiro
Diretor da Direção de Comunicações e Sistemas de Informação do Estado- Maior-General das Forças Armadas (EMGFA)	Brigadeiro-general Carlos Jorge de Oliveira Ribeiro
Diretor do Centro de Investigação da Academia Militar	Professor Doutor Thomas Peter Gasche
Doutorando, investigação em IA	Tenente-coronel Hélder Fernando Ramos do Amaral Parcelas
Diretor do Centro de Investigação Naval	Capitão-de-fragata Jorge Manuel Lourenço Gorricha
Secretário-Geral Adjunto do Ministério da Defesa Nacional	Comodoro Rui Manuel Alves Francisco
Presidente do INESC *Holding*	Professor Doutor Arlindo Oliveira
Chefe da Divisão de Inovação do Estado-Maior da Armada	Capitão-de-fragata João Lourenço da Piedade
Senior Consultant, Industry & Services Solutions, SisTrade	Regina M. Correia
Centro de Investigação da Academia da Força Aérea	Major Luís Filipe da Silva Félix
Diretor Business Development do INOV	Engenheiro John Rodrigues
Chefe da Divisão de Comunicações e Sistemas de Informação do Estado-Maior da Força Aérea	Coronel Bruno Miguel Fernandes Cabaço
Diretor do Departamento de Inovação e Transformação do EMGFA	Brigadeiro-general João Paulo de Almeida
CEO *VisionSpace*	Tiago D. C. Carvalho
Diretora da Direção de Comunicações e Sistemas de Informação, Força Aérea	Coronel Ana Cristina Telha
Principal Engineer, Critical Software	Engenheiro Gonçalo L. Valadas
Subdiretor-Geral de Recursos da Defesa Nacional	Major-general Jorge Filipe Marques Moniz Côrte-Real Andrade
Transportes e Defesa, Indra	Dinis de Oliveira Magalhães
Defence, Security & Space Director, Edisoft	Engenheira Teresa Pires Cardoso
Diretor-geral da Autoridade Marítima e Comandante-geral da Polícia Marítima	Vice-almirante João Dores Aresta

Foi realizado um primeiro contacto, no sentido de aquilatar da disponibilidade da entidade para integrar a investigação, procedendo-se, em seguida e face às anuências, ao agendamento da entrevista. Foram dadas garantias de confidencialidade e anonimato das respostas, de que todas as entidades abdicaram.

Foram elaborados três guiões de entrevista, dois para entidades internas (estrutura do MDN, apenas versando o conceito de IA, e das FFAA, com os dois conceitos estruturantes), e um para externas (apenas o conceito de IA), que foram, depois, revisitados e pontualmente ajustados, com o feedback do coordenador da elaboração da estratégia nacional para a IA em 2019, professor Alípio Jorge.

As respostas às questões colocadas foram analisadas através da frequência de unidades de registo para cada questão, contribuindo uma ou mais questões para cada dimensão do conceito de IA.

Da análise efetuada, extraíram-se observações em cada dimensão do conceito de IA, consideradas como oportunidades e ameaças no âmbito das respostas das entidades externas, extraindo-se das entidades internas as observações consideradas como pontos fortes e pontos fracos, construindo a matriz de suporte à elaboração da análise SWOT.

4. APLICAÇÃO DA IA NO MEIO CIVIL

Neste capítulo, é analisada documentação de referência e entrevistas a entidades externas à luz das seis dimensões definidas – Organização, Progresso, Adoção, Inovação, Dados e Talentos – e respondida a QD1.

4.1. Organização

Das respostas às questões n.º 1.b. (necessidade de materialização em estruturas específicas) e n.º 1.d. (principais *stakeholders*), verifica-se que a postura de ambos os universos externo e interno é semelhante em relação a estruturas, respetivamente 62,5% e 71,4%, valorizando-se a criação de estruturas/unidades orgânicas específicas para fornecerem apoio de forma transversal às áreas da organização na utilização destas tecnologias, designadamente pela vantagem que oferece na obtenção de sinergias entre áreas diferentes (A. Oliveira, entrevista por Teams, 23 de março de 2022), assim como na criação de competências internas e no suporte nestas áreas emergentes às diferentes áreas de negócio (G. L. Valadas, entrevista por E-mail, 31 de março de 2022), onde, em relação a *stakeholders*,

75% referiram as empresas e clientes (O.08)[7] como seus principais *stakeholders* externos, assim como, com 50%, as universidades (Univ), centros de investigação (CInv)/ inovação (CInov) (O.09) e as unidades orgânicas tecnológicas (O.15), tendo sido salientado:

– (swO01): Importância da utilização pelas FFAA da Base Tecnológica e Industrial de Defesa (BTID) como enabling areas, cuja função será criar competências em determinadas áreas tecnológicas e potenciarem a inovação nacional (G. L. Valadas, op. cit.).

Das respostas às questões n.º 2.a. (atividades em curso e/ou projetadas e tecnologias envolvidas) e n.º 2.b. (maior potencial de emprego operacional/em produção), foi possível verificar que a maioria das 18 tecnologias de IA identificadas nas atividades em curso terão potencial de aplicação operacional até 2030, com uma frequência de 75% *Analytic*, 62,5% Apoio à decisão, 50% *Data science*, e 37,5% para *Computer vision*, *Data mining*, *Explainable AI* e Processamento de linguagem natural. Salienta-se com apenas um registo, 12,5%, *AI chips*, *Fuzzy logic*, *Reinforcement learning*, *Safety and security AI*, Simulação e *Supervised learning*, sendo que *Few-shot learning/ Frugal AI*, embora se esteja a trabalhar atualmente, se questiona ainda qual o nível de maturidade tecnológica que será possível alcançar até ao final da década, existindo alguma expetativa quanto ao interesse e mobilização de meios em Portugal para esta área da IA, "onde o Ministério da Defesa, no âmbito da Cyber mas também na vertente do espaço, tem sido muito na vertente científica e de desenvolvimento humano" (T. D. Carvalho, entrevista por Teams, 30 de março de 2022), identificando-se ainda nesta dimensão os seguintes pontos:

– (swO02) A área de *reasoning*, baseada em casos anteriores ou baseada em regras, já tem vindo a ser utilizada em ambiente operacional (G. L. Valadas, *op. cit.)*;

– (swT01) As organizações terão de se preparar para o que encontrarão em 2030-35, pois a atual evolução (código/programas criados por IA daqui a quatro anos e *Exascale computing* a cinco/seis anos) fará com que este seja o timeframe para todos terem acesso a supercomputadores com "inteligência humana" (J. Rodrigues, entrevista presencial, 28 de março de 2022).

[7] Notação utilizada ao longo do trabalho referente a unidade de registo 'O.08', correspondendo a letra à dimensão, neste caso organização (Apêndice D - Quadro 14).

Relativamente aos conceitos de emprego, técnicas, procedimentos e processos envolvendo a adoção de tecnologias de IA, foi possível concluir que 75% possuem documentação específica para a adoção destas tecnologias, sendo que um terço destas entidades o assume com algumas reservas, reconhecendo estar ainda em desenvolvimento ou resultar de trabalhos científicos e necessidades imediatas para transferência de conhecimento (J. Rodrigues, *op. cit.*).

Das respostas à questão n.º 4. (desenvolvimento/manutenção de cultura de inovação), foi possível concluir que todas as entidades afirmam que as suas organizações possuem uma cultura de inovação (I.02), constituindo "uma forma de diferenciação e valorização" (G. L. Valadas, *op. cit.*), sendo que, para 25%, se encontra mesmo na sua génese (I.01), salientando- se os seguintes pontos:

- (swO03) A existência de uma estratégia para a inovação permite envolver membros nos projetos, trazendo motivação e também novos equipamentos (M. L. Proença, entrevista presencial, 15 de março de 2022);
- (swO04) Onde se trabalha conhecimento tecnológico será possível obter RH que muitas vezes se envolvem pelo desafio que lhes é proposto, sendo conveniente ter áreas como núcleos de inovação, com equipas multidisciplinares a que são atribuídos desafios reais de aplicação destas tecnologias (J. Rodrigues, *op. cit.*);
- (swT02) A escassez de pessoas com passaporte da UE e formação académica nestas áreas, associado à morosidade e burocracia do processo de as trazer de fora, tem inflacionado os salários, sendo necessário avaliar como é que a longo prazo este investimento será sustentável, com especial relevância no âmbito do espaço e defesa, onde a maioria do investimento é público (T. D. Carvalho, entrevista por Teams, 30 de março de 2022).

4.5. Dados

Das respostas às questões n.º 5. (obtenção, governação, tratamento e utilização de volume de dados) e n.º 6.a. (preocupações/transformações efetuadas, ou projetadas, para melhor adotar/incorporar tecnologias de IA), no que concerne à postura perante os dados, com uma frequência de 87,5% surge a necessidade de efetuar protocolos/ acordos/ *non-disclosure agreements* (NDA)/ dados dos clientes (D.11), com uma estreita relação entre "parcerias cross-sector" (R. M. Correia, entrevista por Teams, 24 de março de 2022), seguindo-se com 37,5%, a capacidade de ter uma arquitetura flexível (descentralização de dados/ *Cloud*/ servidores

locais) (D.04), a criação de dados sintéticos ou recurso a simulação (D.06), assim como a preocupação com o respeito pelo regulamento geral de proteção de dados (RGPD) e pelas políticas de dados dos parceiros (D.09), sendo que, com 25%, surge a preocupação com as condições de anonimidade dos dados (D.01) e o recurso a dados *open source*. No âmbito das preocupações com vista à preparação para a incorporação das tecnologias de IA, verifica-se com maior frequência, 50%, a referência ao investimento em curso ou planeado em infraestruturas próprias (D.19), com 37,5% das entidades a salientar o estabelecimento de parcerias para acesso a infraestrutura (D.12) e a utilização de infraestruturas/serviços na *Cloud* (D.13), e com uma frequência de 25% para o assegurar competências nas tecnologias / ferramentas atuais (D.14), o garantir comunicações seguras / elevada largura de banda / redundância (D.15) e a existência de poder computacional (D.16), identificando-se nesta dimensão:

– (swO05) A nível de infraestrutura, vantagem de adotar soluções baseadas em serviços na nuvem, não apenas devido às tecnologias de IA, através do acesso a um conjunto de ferramentas que os fornecedores desses serviços disponibilizam, mas também devido à manutenção e evolução da infraestrutura (G. L. Valadas, op. cit.).

4.6. Talentos

Das respostas às questões n.º 1.c. (existência de recursos humanos preparados) e n.º 6.b. (como se poderá preparar melhor ao nível do desenvolvimento de competências específicas para o ciclo de vida da tecnologia), verifica-se que a totalidade tem RH preparados (T.02) para operar com tecnologias de IA, apenas uma entidade, 12,5%, refere explicitamente que são insuficientes (T.03). No que concerne à forma como se poderá preparar melhor, salienta-se a frequência de 37,5% na capacidade de recrutar para novas competências (T.18) e 25% em aposta no business development em inovação (T.06), assegurando a existência de uma equipa competente, que permita, de forma transversal, fazer a ponte entre a tecnologia disponível no mercado e o conhecimento e necessidades funcionais dos clientes (D. O. Magalhães, entrevista por Teams, 05 de abril de 2022), na aposta no ensino e formação (T.08), e em manter estreita relação com academia (T.19). Salienta-se ainda os seguintes pontos:

– (swO06) Constituir uma comunidade IA promovendo a troca de conhecimento e de experiência entre pares (T. P. Cardoso, entrevista presencial, 05 de abril de 2022);

– (swT03) O ciclo de vida da tecnologia tem vindo a decrescer a uma velocidade crescente, fazendo com que também os requisitos operacionais se alterem durante o período de desenvolvimento da tecnologia (G. L. Valadas, op. cit.).

4.7. Síntese conclusiva

Da análise efetuada, e em resposta à QD1, *Como é que a IA é aplicada no meio civil?*, conclui-se que em Portugal, designadamente no meio cívil, esta aplicação passa por:

- recurso a pessoas com competências, apesar do reconhecimento da escassez de oferta;
- adoção de uma postura que procura acompanhar as dinâmicas e desafios colocados por estas tecnologias de IA nas diferentes dimensões, salientando-se a valorização de estruturas específicas para apoio à criação de competências e o estabelecimento de parcerias, com academia e centros de inovação;
- existência de abrangente experiência em *data analytics* e *reasoning*, utilizada em ambiente operacional, e proficiência noutras tecnologias, como *data science*, *computer vision*, *data mining*, *explainable AI* e processamento de linguagem natural;
- reconhecimento da relevância atual da cultura de inovação nas organizações, como indutor de motivação e catalisador de recursos; e
- necessidade de assegurar o acesso a dados ao abrigo de protocolos e estabelecimento de NDA.

5. APLICAÇÃO DA IA EM OPERAÇÕES MILITARES DAS FFAA PORTUGUESAS

Neste capítulo, é analisada documentação de referência e entrevistas a entidades internas à luz das seis dimensões definidas para o conceito de IA – Organização, Progresso, Adoção, Inovação, Dados e Talentos –, bem como das dimensões definidas para o conceito de OpMil – manobra, fogos, C2, informações, atividades de informação, apoio logístico, proteção da força e CIMIC –, e respondida a QD2.

5.1. Organização

No que toca à documentação estruturante, materialização de estruturas específicas e principais stakeholders,verificou-se, ao nível da "tradução" em documentação estruturante, uma frequência de 50% em concordância[8] (O.01), 42,8% dos quais (três em sete) referem documentos resultantes de trabalhos científicos e candidaturas a projetos (O.03), registando-se que 46,2% não possuem (O.04) e que 14,3% tem documentação em produção (O.02). Em relação à necessidade de se materializar em estruturas/unidades orgânicas específicas (O.05), com uma postura semelhante às entidades externas, regista-se uma concordância ligeiramente superior internamente, com 71,4% (face aos 62,5%), assinalando-se ainda a relevância atribuída à liderança executiva (O.11) como *stakeholder*, com uma frequência de 71,4%, tendo 42,9% destacado as Univ/ CInv/ CInov (O.09), 35,7% o MDN (O.07) e 28,6% a BTID (O.08), extraindo-se ainda os seguintes pontos:

- (swS01) Vantagem da existência de estrutura de acompanhamento e coordenação do esforço e do investimento nestas áreas (EA-IDEIA - Investigação, Desenvolvimento, Experimentação e Inovação da Armada) (J. M. Gorricha, entrevista por Teams, 21 de março de 2022);
- (swS02) Potencial decorrente da publicação da Diretiva Estratégica para a Inovação das FFAA (L. F. Félix, entrevista por Teams, 25 de março de 2022);
- (swW01) Necessidade de enquadramento e orientação para incrementar a coordenação de esforços nas FFAA (H. F. Parcelas, entrevista por Teams, 18 de março de 2022).

5.2. Progresso

Foi possível verificar que os projetos nas FFAA, em curso ou planeados, com capacidade operacional até 2030, envolvem dez das 18 tecnologias abordadas pelas entidades externas, registando-se três tecnologias com uma frequência de 50%: Apoio à decisão (*open source*); Apoio à decisão (*reasoning*); e *Computer vision*. Assinala-se ainda as tecnologias *Analytics* com 42,9%, *Data science* e Sistemas preditivos com 35,7%, correspondendo às restantes, *Data mining*, Robótica e Simulação uma frequência de 14,3%, e Processamento de linguagem natural com

[8] As FFAA portuguesas apresentaram a sua Diretiva Estratégica para a Inovação em fevereiro de 2022 (EMGFA, 2022), onde a exploração de aplicações de IA e a sua integração na edificação de capacidades para as FFAA se encontra expressa numa das suas LA.

7,1%, identificando-se ainda os seguintes pontos:

- (swS03) As FFAA, enquanto parceiros da BTID, poderão dar um contributo válido e precioso através da definição de requisitos técnicos e operacionais (H. F. Parcelas, *op. cit.*);
- (swW02) Necessidade de construir uma consciência global relativa às capacidades da IA ao nível estratégico e operacional (H. F. Parcelas, *op. cit.*);
- (swW03) Necessidade de alcançar as condições prévias habilitantes da incorporação destas tecnologias em operação (A. C. Telha, entrevista presencial, 31 de março de 2022);
- (swW04) Necessidade de explorar a área da manutenção preditiva, complementarmente com manufatura aditiva (envolvendo a impressão 3D) (J. L. Piedade, entrevista presencial, 23 de março de 2022).

5.3. Adoção

Das respostas à questão n.º 3., foi possível concluir que 85,7% não possui documentação específica (A.01) com vista à adoção destas tecnologias, designadamente conceitos de emprego, técnicas e procedimentos, sendo as exceções, 14,3%, embora assumindo com algumas reservas (A.03), áreas específicas na Secretaria-Geral do Ministério da Defesa Nacional (R. M. Francisco, entrevista presencial, 22 de março de 2022) e na Marinha (J. L. Piedade, *op. cit.*), demonstrando existência de caminho a percorrer nesta área para a adoção operacional destas tecnologias.

5.4. Inovação

Todas as entidades afirmam que as suas organizações possuem uma cultura de inovação, sendo inclusivamente enfatizado que "quem não tem uma visão inovadora e de desenvolvimento estará sempre um passo atrás das demais congéneres" (J. D. Aresta, entrevista por e-mail, 22 de abril de 2022), salientando 50% das entidades a existência e /ou criação de estruturas de inovação, 14,3% a realização de seminários / conferências / roadshows e 7,1% a participação / organização de exercícios, salientando-se:

- (swS04) Capacidade de alinhamento de projetos com plano de Investigação, Desenvolvimento e Inovação (ID&I), encorajada através da avaliação, função dos critérios definidos em diretiva própria, e respetiva atribuição de financiamento (T. P. Gasche, entrevista presencial, 18 de março de 2022);

– (swS05) Realização de eventos para promover condições de *networking*, designadamente através de *roadshow*, indo ao encontro do que melhor se faz em Portugal nas tecnologias identificadas pela OTAN e UE, procurando partilhar ideias e intenções, e incrementar o conhecimento mútuo (J. L. Piedade, *op. cit.*);
– (swS06) Projeto para construção de constelação de centros de inovação, investigação e desenvolvimento, constituindo-se no Centro de Investigação Naval o CINAVLab como um dos pilares desta constelação (J. M. Gorricha, *op. cit.*);
– (swS07) Programa de incentivo aos militares para continuarem estudos por via de doutoramento (L. F. Félix, *op. cit.)*;
– (swW05) Necessidade de generalização da cultura de inovação (L. M. Calmeiro, entrevista presencial, 15 de março de 2022);
– (swW06) Inexistência de uma linha de esforço, ou orientação, que permita devolver à organização os ensinamentos e desenvolvimentos efetuados no âmbito de trabalhos, estudo e teses (H. F. Parcelas, *op. cit.*);
– (swW07) Limitações em termos de RH, que já de si apresenta dificuldades ao nível das qualificações, condicionam a capacidade de olhar para lá do horizonte atual (R. M. Francisco, *op. cit.*);
– (swW08) Necessidade de recrutar para as necessidades atuais (B. M. Cabaço, entrevista presencial, 29 de março de 2022);
– (swO07) Futura criação do *Hub for European Defence Innovation* na Agência Europeia de Defesa (J. F. Côrte-Real Andrade, entrevista presencial, 04 de abril de 2022).

5.5. Dados

Das respostas às questões n.º 5. e 6.a., da gestão e postura perante dados, de uma forma transversal, constata-se que se está no início e a promover a adoção de IA de forma muito controlada, essencialmente centrada em ilhas de inovação e conhecimento (P. F. Nunes, entrevista presencial, 14 de março de 2022), registando-se uma frequência de 64,3% na identificação da necessidade de efetuar protocolos/ acordos/ NDA (D.11), sendo necessário incrementar os mecanismos para, nestas tecnologias, potenciar a utilização conjunta em IA dos dados existentes nos diferentes centros de dados dos ramos, criando "massa crítica" neste campo, com 21,4% referindo a capacidade de utilização de dados próprios e a preocupação com o respeito pelo RGPD. No âmbito das preocupações referentes a transformações

necessárias à adoção destas tecnologias, destaca-se com uma frequência de 42,9% o investimento em curso ou planeado em infraestruturas próprias, seguindo-se com 21,4% a existência de poder computacional e a preocupação com a incorporação de requisitos orientados a IA nos processos aquisitivos, salientando-se:

- (swS08) Capacidade de dados próprios do Centro de Dados da Defesa (CDD) (R. M. Francisco, *op. cit.*);
- (swW09) Necessidade de adoção prévia de ferramentas de *data curation* para futura utilização de dados para a tomada de decisão (P. F. Nunes, *op. cit.*);
- (swW10) Necessidade de elevar o nível de preocupação em relação ao impacto no ciclo de vida dos dados (C. J. Ribeiro, entrevista presencial, 17 de março de 2022);
- (swW11) Necessidade de abordar a temática dos dados de forma mais estruturada e centralizada (J. P. Almeida, entrevista presencial, 29 de março de 2022);
- (swW12) Necesidade de um centro de cálculo (T. P. Casche, *op. cit.*);
- (swW13) Necessidade de RH com competências para melhor aproveitamento dos dados disponíveis (R. M. Francisco, *op. cit.;* B. M. Cabaço, *op. cit.*);
- (swW14) Necessidade de implementação das interfaces que assegurem a interoperabilidade necessária para acesso a diferentes fontes de dados (R. M. Francisco, *op. cit.*);
- (swW15) Dificuldade de transferência e atualização de dados entre serviços do Estado (J. F. Côrte-Real Andrade, *op. cit.*);
- (swT04) Atraso ou não transposição para Portugal da Legislação Europeia que visa melhorar a capacidade de transferência e atualização de dados entre serviços do Estado (J. F. Côrte-Real Andrade, *op. cit.*).

5.6. Talentos

Das respostas às questões n.º 1.c e 6.b., resulta que 57,1% refere ter RH preparados para operar com tecnologias de IA (T.02), 87,5% (sete em oito) dos quais considera insuficientes (T.03), sendo necessário encontrar soluções para potenciar os núcleos de pessoas com competências, com desafios para maior interação ao nível da experimentação de nível operacional conjunto, relacionando com a dimensão dados, não apenas na área académica, verificando-se 28,6% como assumindo não

ter (T.01). Referente à forma como preparar melhor ao nível do desenvolvimento de competências, verifica-se a frequência de 64,3% na aposta no ensino e formação (T.08), dos quais 55,6% (35,7% do total) salientam a formação transversal em sistemas de informação / tecnologias de informação e comunicações (T.08.1) e 44,4% (28,6% do total) a formação transversal sobre tecnologias de IA (T.08.2), seguindo-se com 14,3%, o apoio à investigação (doutoramentos/ doutorados) (T.04), o assegurar formação regular às áreas tecnológicas (T.08.3) e a gestão de carreira específica para a IA (T.15), salientando-se:

- (swS09) Existência de pessoas com competências para, com especialização adicional, poderem abraçar os desafios inerentes à adoção de tecnologias de IA (H. F. Parcelas, *op. cit.*);
- (swW16) Necessidade de criação prévia de use cases com vista a promover a obtenção dos *quick wins* necessários para promover a aplicação destas tecnologias (P. F. Nunes, *op. cit.*);
- (swW17) Necessidade de criar um *skill set* para lidar com as tecnologias de IA no âmbito de toda a organização (P. F. Nunes, *op. cit.*);
- (swW18) Necessidade de estruturar de forma mais coerente, ao nível da defesa nacional, a abordagem a estas áreas das tecnologias emergentes (R. M. Francisco, *op. cit.*);
- (swW19) Apesar de se possuir pessoas com capacidades, não se consegue usufruir devidamente em retorno do investimento, designadamente nos militares (T.P. Gasche, *op. cit.*);
- (swW20) Capacidade de retenção de RH nas FFAA (B. M. Cabaço, *op. cit.*).

5.7. Análise referente à IA no âmbito do conceito de operações militares.

Apresenta-se nos pontos seguintes a análise referente ao conceito de OpMil, incluindo-se os participantes a prestar serviço nas estruturas do EMGFA e dos ramos.

5.7.1. Processos/sistemas com potencial para incorporação de IA

Foi possível verificar que a maioria dos participantes identificou pelo menos um processo/ sistema por dimensão (função de combate) com potencial para incorporar tecnologias de IA, sendo que se registou uma frequência de 100% para

as dimensões C2, Informações e Apoio logístico, 90,9% CIMIC, 72,7% Manobra, e 63,6% Fogos, observando-se a menor frequência, com 45%, em Atividades de informação e Proteção da força, evidenciando-se nestas últimas alguma dificuldade em identificar processos/sistemas com potencial para beneficiar das vantagens da incorporação de tecnologias de IA.

Da análise em função da frequência por unidade de registo, correspondentes às áreas de maior impacto identificadas pela OTAN (matrizes de unidade de contexto e de registo), efetuada para determinação da ordem de desempate na ordenação preferencial dentro de cada dimensão, foi possível concluir que cerca de três quartos do total dos participantes na investigação identificaram processos/sistemas associados às áreas C4ISR, Apoio à Decisão e Gestão, Veículos Autónomos e Planeamento de Capacidades, as duas primeiras com uma frequência de 27% e as restantes com 10,3%, sendo que Treino (2,4%), Apoio Sanitário (0,8%) e NBQR (0,8%) foram as áreas onde as entidades entrevistadas encontraram maior dificuldade em identificar processos/sistemas a elas associadas com potencial para beneficiar da incorporação de tecnologias de IA até ao final da década.

5.7.2. Prioridades de investimento por funções de combate

Foi estabelecida a ordenação das prioridades que se apresenta no Quadro 7, verificando-se que as três dimensões com 100% de frequência de respostas foram as que obtiveram maior grau de prioridade (valor mais baixo), com a seguinte ordenação: C2, Informações e Apoio logístico. As duas primeiras são coincidentes com as primeiras prioridades do ExEsp, o que poderá ser potenciador de eventuais cooperações e parcerias futuras, designadamente no âmbito de projetos europeus.

Tabela 5 – Ordenação preferencial por funções de combate com base nas respostas à questão n.8.

Ordenação	Dimensão
1	C2
2	Informações
3	Apoio logístico
4	Manobra
5	Atividades de informação
6	CIMIC
7	Proteção da força
8	Fogos

Através dos processos/sistemas identificados por cada entidade na questão n.º 7., utilizou-se o processo de ordenação preferencial para determinar as prioridades pelas áreas de impacto correspondentes nas três dimensões prioritárias, C2, Informações e Apoio Logístico, resultando a ordenação que se apresenta no Tabela 6.

Tabela 6 – Ordenação das áreas de maior impacto da IA

Dimensão	Ordenação	Área
C2	1	Apoio à Decisão e Gestão
	2	C4ISR
	3	Veículos Autónomos
	4	Ciberespaço e espaço informacional
	5	Armas e Efeitos
	6	Planeamento de Capacidades
Informações	1	C4ISR
	2	Apoio à Decisão e Gestão
	3	Ciberespaço e espaço informacional
	4	Veículos Autónomos
Apoio logístico	1	Logística
	2	Apoio à Decisão e Gestão
	3	Veículos Autónomos
	4	Planeamento de Capacidades
	5	C4ISR

Encontram-se referenciadas no quadro anterior sete das dez áreas identificadas pela OTAN, demonstrando alinhamento e potencial para parcerias internacionais futuras, concluindo-se a seguinte prioridade atribuída por dimensão para incorporação de tecnologias de IA a processos e sistemas de:

– C2: Apoio à Decisão e Gestão; C4ISR e Veículos Autónomos;

– Informações: C4ISR, Apoio à Decisão e Gestão e Ciberespaço;

– Apoio Logístico: Logística, Apoio à Decisão e Gestão e Veículos Autónomos.

5.8. Alinhamento com a estratégia nacional para a IA e análise SWOT.

As áreas prioritárias identificadas encontram-se englobadas na estratégia nacional definida em 2019, designadamente nas áreas de especialização em Portugal "Tomada de decisão em Tempo Real com IA" e "IA para computação de

ponta", com as áreas de pesquisa e inovação em redes europeias e internacionais "CiberSegurança" e com pesquisa fundamental para a IA do Futuro "IA autónoma" e "AutoML", alinhamento reforçado pelo facto de se concluir que as FFAA desenvolvem projetos envolvendo, ou com previsão de o fazer com potencial da sua utilização operacional até 2030, dez das 18 tecnologias de IA referenciadas pelas entidades externas nacionais.

Com base na análise efetuada, extraíram-se pontos fortes e pontos fracos, assim como, no capítulo anterior, se salientaram oportunidades e ameaças, obtendo-se um conjunto de contributos resultantes da construção da matriz SWOT, na sua variante TOWS (Visual Paradigm, s.d.), procurando-se potenciar as oportunidades com os pontos fortes (swSO) e minimizar as ameaças tirando partido das oportunidades (swWO), assim como minimizar as ameaças recorrendo aos pontos fortes identificados (swST) e evitar ameaças minimizando os pontos fracos (swWT), conforme se apresenta no Quadro 9.

Quadro 9 – Conceito de IA (análise SWOT, apresentada na variante TOWS)

		Ambiente Interno (MDN e FFAA)	
		Pontos Fortes (swS)	Pontos Fracos (swW)
Ambiente Externo (meio civil)	Oportunidades (swO)	swSO	swWO
		swSO1: swS01/swS02/swS04/swO03; swSO2: swS05/swS07/swS08/swO04; swSO3: swS06/swO05; swSO4: swS09/swO06; swSO5: swS01/swS02/swS03/swO07.	swWO1: swW16/swW17/swO01; swWO2: swW04/swW7/swO02; swWO3: swW02/swW10/swW11/swW18/swO03; swWO4: swW13/swW20/swO04; swWO5: swW12/swO05; swWO6: swW03/swW09/swO06
	Ameaças (swT)	swST	swWT
		swST1: swS01/swS02/swT01; swST2: swS7/swS09/swT02; swST3: swS3/swT03.	swWT1: swW10/swW11/swT01; swWT2: swW7/swW19/swW20/swT02; swWT3: swW14/swW15/swT04.

5.9. Síntese conclusiva

Através da análise efetuada, e em resposta à QD2, *Qual a aplicação da IA em OpMil nas FFAA portuguesas? c*onclui-se que esta aplicação se manifesta da seguinte forma:

– postura proativa de transformação e evolução na área de inovação, onde a diretiva estratégica para a inovação nas FFAA assume particular relevância;

- valorização de estruturas específicas para apoio à criação de competências em tecnologias emergentes e disruptivas, onde a Marinha apresenta maior experiência e conhecimento adquirido;
- elevada relevância atribuida ao decisor executivo enquanto *stakeholder*;
- envolvimento das diferentes estruturas das FFAA em projetos com dez das 18 tecnologias identificadas pelas entidades externas como possuindo potencial de utilização operacional até 2030, destacando-se as de apoio à decisão (*reasoning*), *computer vision*, e apoio à decisão (*open source*);
- reconhecimento da necessidade de estabelecimento de protocolos e NDA para aceder a dados, apesar da vantagem que o CDD apresenta neste particular, sendo necessário potenciar a utilização conjunta em IA dos dados existentes nos diferentes centros de dados dos ramos, criando "massa crítica" neste campo;
- necessidade de incrementar o conhecimento genérico sobre tecnologias de IA e, no particular, para o desenvolvimento de documentação especifica referente ao emprego destas tecnologias de IA;
- assunção de que são insuficientes as pessoas que constituem os núcleos com competências para abarcar estas tecnologias, sendo igualmente necessário encontrar soluções para potenciar estes núcleos, designadamente com desafios para maior interação ao nível da experimentação de nível operacional conjunto, relacionado com a necessidade de potenciar os dados a nível conjunto, não apenas na área académica; e
- consideração do C2, Informações e Apoio Logístico como as funções de combate prioritárias, na perspetiva de incorporação e utilização de tecnologias de IA com vista à sua operação até 2030, envolvendo as áreas de Apoio à Decisão e Gestão, C4ISR, Veículos Autónomos, Ciberespaço e espaço informacional, Armas e Efeitos, Planeamento de Capacidades e Logística.

Apresenta-se no capítulo seguinte o conjunto de contributos derivados da análise SWOT.

5.10. Proposta de contributos para a aplicação de IA em operações militares, e resposta à questão central

Decorrente do até aqui analisado, e em resposta à QC: *Como melhorar a capacidade de exploração das tecnologias de IA em operações militares pelas FFAA*

portuguesas?, conclui-se que as diferentes estruturas das FFAA se encontram envolvidas em dez das 18 tecnologias identificadas pelas entidades externas participantes na investigação, de onde se destacam as de apoio à decisão (*reasoning*), *computer vision*, e apoio à decisão (*open source*), existindo uma postura proativa de transformação e evolução na área de inovação mas existindo, no âmbito específico das tecnologias de IA e da sua aplicação na perspetiva de emprego em OpMil até ao final da década, a necessidade de evoluir de forma célere em diferentes dimensões, conforme se apresenta na proposta de contributos da Tabela 7.

Tabela 7 – Contributos para melhorar a postura das FFAA na adoção de tecnologias IA

#	Proposta (conforme matriz do Quadro 9)	Dimensão
swSO1	Criar mecanismos próprios de financiamento (Call ID&I FFAA) em linha de investigação específica para projetos conjuntos com recurso a tecnologias de IA nas áreas propostas como prioritárias.	Organização; Inovação
swSO2	Incrementar os eventos para uma promoção proativa do potencial das FFAA, integrando os três ramos, no apoio a projetos com tecnologias de IA, e procura de conhecimento, junto dos centros de inovação nacionais nas áreas propostas como prioritárias.	Inovação
swSO3	Potenciar a adoção de tecnologias de IA através da constituição de capacidade supletiva nos Centros de Dados das FFAA, incluindo a contratação de serviços na nuvem.	Dados
swSO4	Construir uma comunidade específica de IA das FFAA, com coordenação do Departamento para a Inovação e Transformação do EMGFA e serviços digitais de suporte assegurados pelo EMGFA.	Talentos
swSO5	Intensificar o estabelecimento de parcerias entre as FFAA e suas congéneres de países da UE com vista à obtenção de financiamento supletivo para projetos que envolvam tecnologias de IA nas áreas propostas como prioritárias.	Inovação
swWO1	Incrementar o recurso à contratação de serviços ao Sistema Científico e Tecnológico Nacional e à BTID.	Organização
swWO2	Desenvolver estudos com o foco na análise de incorporação de tecnologias de IA no âmbito da manutenção preditiva em OpMil, complementarmente com a capacidade de utilização de manufatura aditiva, em particular por Forças Nacionais Destacadas.	Progresso
swWO3	Desenvolver eventos conjuntos para divulgação interna do potencial das FFAA para apoio a projetos com tecnologias de IA.	Inovação
swWO4	Incentivar a criação de desafios de inovação formais com adoção de tecnologias de IA nas unidades orgânicas das FFAA com capacidade de desenvolvimento de software.	Inovação
swWO5	Avaliar o desenvolvimento de parcerias ao nível das FFAA com o Sistema Científico e Tecnológico Nacional (SCTN) com vista a estabelecimento de protocolos de acesso a infraestruturas de computação.	Dados
swWO6	Desenvolver um *roadmap* para a aplicação de tecnologias de IA até 2030 nas áreas propostas como prioritárias.	Adoção; Talentos

[Cont.]

swST1	Elaborar uma Diretiva Estratégia para a aplicação das tecnologias de IA nas FFAA.	Adoção; Organização
swST2	Incrementar os apoios, tanto financeiros como organizacionais, para promover a continuação de estudos de doutoramento por militares dos quadros permanentes nas áreas das tecnologias disruptivas.	Progresso
swST3	Incrementar a interação via workshops temáticos com a BTID, envolvendo a apresentação regular pela indústria nacional das tecnologias de IA que consideram ter potencial de aplicação em sistemas militares.	Talentos
swWT1	Desenvolver estudos para identificar os mecanismos necessários à transformação no ciclo de vida dos dados nas FFAA enquanto recurso chave das tecnologias de IA.	Organização
swWT2	Desenvolver estudos referentes à atratividade e capacidade de retenção nas FFAA dos militares dos quadros permanentes com competências específicas nas engenharias.	Talentos
swWT3	Elaborar um estudo, ao nível do MDN, com vista à avaliação do impacto resultante do atraso na transposição da legislação da UE no âmbito da transferência e atualização de dados entre serviços do Estado, assente em estudos de caso na área da mobilização e reserva de disponibilidade.	Dados

Apresenta-se na Tabela 8 a proposta para efeitos de priorização de esforço de investimento de incorporação de tecnologias de IA em processos/sistemas das FFAA, no âmbito das três funções de combate consideradas como prioritárias.

Tabela 8 – Contributos para priorização das áreas de incorporação de tecnologias IA

Função de Combate (ordem de prioridade)	Prioridade	Área de impacto das tecnologias de IA
1. Comando e Controlo	1	Apoio à decisão e gestão
	2	C4ISR
	3	Veículos autónomos
	4	Ciberespaço e espaço informacional
	5	Armas e efeitos
	6	Planeamento de capacidades
2. Informações	1	C4ISR
	2	Apoio à Decisão e Gestão
	3	Ciberespaço e espaço informacional
	4	Veículos Autónomos

[Cont.]

3. Apoio logístico	1	Logística
	2	Apoio à Decisão e Gestão
	3	Veículos Autónomos
	4	Planeamento de Capacidades
	5	C4ISR

6. CONCLUSÕES

De uma forma global, a evolução tecnológica atual e a forte convergência do *big data*, do poder computacional e da investigação em algoritmos de *machine learning* – concentrando-se a liderança do conhecimento e a definição de tendências de evolução para as tecnologias emergentes e disruptivas como a IA essencialmente na sociedade civil –, constitui um desafio em termos de Segurança e Defesa.

A exiguidade de RH nas FFAA acresce a este desafio, designadamente em função da crescente complexidade dos sistemas de armas e da necessidade de assegurar em permanência a sua sustentação e condição de operacionalidade.

As tecnologias de IA possuem um caráter estruturante que irá provavelmente afetar todo o espectro de atividades, conforme reconhecem os países que integram a OTAN, constituindo a sua aplicação um real fator multiplicador de força, transversal aos diferentes domínios operacionais.

Na perspetiva da execução de tarefas que incrementam (*augment*) a inteligência humana, a incorporação de tecnologias de IA em processos/sistemas operacionais, em particular algoritmos de aprendizagem, tem-se revelado um importante auxílio e desempenhado um crescente papel no campo de batalha, designadamente através da implementação de mecanismos de previsão e da sua consequente possibilidade de atuação por antecipação.

Metodologicamente, esta investigação assentou num raciocínio indutivo, associado a uma estratégia qualitativa, e um desenho de pesquisa do tipo estudo de caso.

Neste âmbito, em resposta ao OE1, *Analisar a aplicação da IA no meio civil*, e associada QD1, tendo por base a análise documental e de conteúdo de oito entrevistas, concluiu-se que esta aplicação é caracterizada pela(o): existência

de abrangente experiência em d*ata analytics* e *reasoning*, utilizada em ambiente operacional, e proficiência noutras tecnologias, como *data science, computer vision, data mining, explainable AI;* assegurar da capacidade de recorrer a pessoas com competências, apesar da escassez de oferta; reconhecimento da relevância atual da cultura de inovação nas organizações, enquanto indutor de motivação e catalisador de recursos; acompanhamento das dinâmicas e desafios colocados por estas tecnologias de IA nas diferentes dimensões, com a valorização de estruturas específicas para apoio à criação de competências e o estabelecimento de parcerias, designadamente com academia e centros de inovação; e a necessidade de assegurar o acesso a dados ao abrigo de protocolos e NDA.

Cumprindo com o OE2, *Analisar a aplicação da IA em OpMil nas FFAA portuguesas,* e com a correspondente QD2, tendo por base a análise documental e de conteúdo de 14 entrevistas, concluiu-se que a sua aplicação se caracteriza: pelo envolvimento em projetos internos às FFAA com potencial de utilização de tecnologias de IA, designadamente dez das 18 tecnologias identificadas por entidades externas como possuindo potencial para poderem vir a ser utilizadas até 2030 em contexto operacional, de entre as quais se destacam as de apoio à decisão (*reasoning), computer vision*, e apoio à decisão (*open source*); por uma postura proativa de transformação e evolução na área de inovação; pela valorização de estruturas específicas para apoio à criação de competências em tecnologias emergentes e disruptivas, como as de IA; pela elevada relevância atribuída ao decisor executivo enquanto *stakeholder*; pelo reconhecimento da necessidade de estabelecer protocolos e NDA para aceder a dados; pela necessidade de incrementar o conhecimento genérico sobre tecnologias de IA e, no particular, para desenvolvimento de documentação especifica referente ao emprego destas tecnologias de IA; e pelo reconhecimento de que as pessoas que constituem os núcleos com competências para abarcar estas tecnologias são insuficientes.

Concluiu-se, ainda, que as funções de combate C2, Informações e Apoio logístico, na ordem referida, são consideradas prioritárias para a sua incorporação, na perspetiva de utilização destas tecnologias de IA em operação até ao final da década, envolvendo as áreas de Apoio à decisão e gestão, C4ISR, Veículos autónomos, Ciberespaço e espaço informacional, Armas e efeitos, Planeamento de capacidades e Logística.

Pelo referido, e em resposta ao OG, *propor contributos para melhorar a exploração das tecnologias de IA em operações militares pelas FFAA portuguesas,*

e correspondente QC, concluiu-se que estes passam pela implementação de 17 propostas concernentes à postura perante as tecnologias de IA, nas dimensões:

– Organização, pela criação de mecanismos próprios de financiamento (*Call ID&I* das FFAA) em linha de investigação específica para IA, incremento do recurso à contratação de serviços ao SCTN e BTID, e desenvolver estudos para identificar as necessárias transformações no ciclo de vida dos dados enquanto recurso chave no contexto da IA;

– Progresso, através da incorporação de tecnologias de IA para manutenção preditiva em OpMil, em particular por Forças Nacionais Destacadas, e do incremento de apoios para estudos de doutoramento por militares dos quadros permanentes em tecnologias disruptivas;

– Adoção, mediante o desenvolvimento de uma Diretiva Estratégica para a IA nas FFAA, e de um roadmap para a sua aplicação até 2030 nas áreas prioritárias propostas;

– Inovação, através do incremento de eventos para uma promoção proativa do potencial das FFAA, integrando os três ramos, no apoio a projetos com tecnologias de IA, e procura de conhecimento, junto dos centros de inovação nacionais nas áreas propostas como prioritárias, da intensificação do estabelecimento de parcerias entre as FFAA e suas congéneres de países da EU com vista à obtenção de financiamento supletivo para projetos nas áreas propostas como prioritárias, e do incentivo à criação de desafios de inovação com adoção de tecnologias de IA nas áreas de desenvolvimento de software das FFAA e desenvolver eventos para divulgação interna do potencial das FFAA;

– Dados, mediante a criação de capacidade supletiva nos centros de dados das FFAA por forma a potenciar a adoção de IA, incluindo a contratação de serviços na nuvem, da avaliação do desenvolvimento de parcerias com o SCTN para acesso a infraestruturas de computação, e da elaboração de estudo ao nível do MDN, referente o impacto do atraso na transposição de legislação da UE no âmbito da transferência e atualização de dados entre serviços do Estado;

– Talentos, mediante a construção de uma comunidade de IA nas FFAA, com coordenação do Departamento para a Inovação e Transformação do EMGFA, do incremento da interação regular com a BTID em workshops temáticos envolvendo apresentação de tecnologias de IA que consideram ter potencial de aplicação em sistemas militares e desenvolvimento de estudos relativos à capacidade de retenção e atratividade no âmbito das engenharias.

O estudo apresenta como principal **contributo para o conhecimento** a formulação de um conjunto de propostas, metodológica e cientificamente validadas, para melhorar a capacidade das FFAA na exploração de tecnologias de IA e no alcançar de maturidade tecnológica para o seu emprego operacional (no horizonte de até 2030).

As duas principais **limitações**, alheias à investigação e que, contudo, não condicionaram a mais-valia das evidências encontradas, associam-se a sobreposições e interdependências tecnológicas abordadas e à sua associação com as funções de combate.

Em matéria de **estudos futuros** sugere-se a análise focada na incorporação de tecnologias de IA no âmbito da manutenção preditiva em apoio às Forças Nacionais Destacadas.

REFERÊNCIAS BIBLIOGRÁFICAS

Agência para a Modernização Administrativa. (s.d.). *Guia para uma Inteligência Artificial ética, transparente e responsável na administração pública*. Retirado de https://tic.gov.pt/documents/37177/293193/GuIA+Responsa%CC%81vel+para+a+IA+na+AP.pdf/b7b73227-7750-f6eb-a3a8-21bfd97d1e40

Comissão Europeia. (s.d.). AI Watch Investments: AI investments in the EU member states [Online]. Retirado de https://web.jrc.ec.europa.eu/dashboard/AI_WATCH_INVESTMENTS/index.html? bookmark=member_states

Conselho de Chefes de Estado-Maior. (2014a), *Conceito Estratégico Militar* [Aprovado pelo MDN em 22 de julho de 2014, confirmado pelo CSDN de 30 de julho de 2014]. Lisboa: Ministério da Defesa Nacional.

Conselho de Chefes de Estado-Maior. (2014b). *Missões das Forças Armadas* (MIFA) [Aprovado em CSDN em 30 de julho de 2014]. Lisboa: Ministério da Defesa Nacional.

Conselho Europeu. (2020). *Ad hoc Committee on Artificial Intelligence (CAHAI)*. Retirado de https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da

Cooperative Cyber Defence Centre of Excellence. (2021). *AI and Autonomy in the Military: An Overview of NATO Member States' Strategies and Deployment*. Retirado de https://ccdcoe.org/uploads/2021/12/Strategies_and_Deployment_A4.pdf

Costa, P. (2020). Aplicação da Inteligência Artificial no domínio da Segurança e Defesa. Em: L.E. Saraiva & S. Fernandes (Coords.) (2020). *Após as novas guerras: Repensar a violência em Relações Internacionais,* (167-184). Coleção "ARES", 35. Lisboa: Instituto Universitário Militar.

Domingos, P. (2015). *The Master Algorithm*. EUA: Penguin Books.

Estado-Maior do Exército. (2012). *PDE 3-00 Operações*. Lisboa: Estado-Maior do Exército.

Estado-Maior-General das Forças Armadas. (2022). *Diretiva Estratégica para a Inovação nas Forças Armadas 2022 – 2032* [Versão de 15 de janeiro de 2022]. Lisboa: Estado-Maior-General das Forças Armadas.

Exército da Alemanha. (2019). *Artificial Intelligence in Land Forces*. [Online]. Retirado de https://www.bundeswehr.de/resource/blob/156026/79046a24322feb96b2d8cce168315249/download-positionspapier-englische-version-data.pdf

Exército de Espanha. (2019). *Fuerza 35*. [Página *online*]. Retirado de http://www.ejercito.mde.es/Galerias/Descarga_pdf/EjercitoTierra/Publicaciones/fuerza_35.pdf

Governo de Espanha. (2020). *Estrategia Nacional de Inteligencia Artificial*. [Página *online*]. Retirado de https://www.lamoncloa.gob.es/presidente/actividades/Documents/2020/021220- ENIA.pdf

Governo do Reino Unido. (2021), *National AI Strategy*. [Online]. Retirado de https ://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1020402/National_AI_Strategy_-_PDF_version.pdf

Governo Federal da Alemanha. (2018). *Artificial Intelligence Strategy*. [Online]. Retirado de https://www.ki-strategie- deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf

Iniciativa Integrada de Política Pública Dedicada ao Reforço de Competências Digitais. (2019). AI Portugal 2030: Portuguese national initiative on digital skills. Retirado de https://www.incode2030.gov.pt/sites/default/files/julho_incode_brochura.pdf

Iniciativa Integrada de Política Pública Dedicada ao Reforço de Competências Digitais. (2020). Indicadores – O Observatório das Competências Digitais [Online]. Retirado de https://observatorio.incode2030.gov.pt/indicadores/indicadores-todos- por-eixos-de-acao/

Iniciativa Integrada de Política Pública Dedicada ao Reforço de Competências Digitais. (2021). AI Portugal 2030 [Página *online*]. Retirado de https://www.incode2030.gov.pt/ai-portugal--2030

Kanaan, M. (2020). *T-Minus AI*. Dallas: BenBella Books, Inc.

Kepner, J., & Gadepally, V. (2020). *Mathematics of Big Data and Machine Learning – Session 1 Artificial Intelligence and Machine Learning* [Sessão MIT Lincoln Laboratory]. Retirado de https://www.youtube.com/watch?v=t4K6lney7Zw

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C.E. (1955). A Proposal For The Dartmouth Summer Research Project On Artificial Intelligence [Página *online*]. Retirado de http://www-formal.stanford.edu/jmc/history/dartmouth/dartmouth.html

Ministério da Defesa de França. (2019). *Artificial Intelligence In Support Of Defence - Report of the AI Task Force*. Retirado de https://www.defense.gouv.fr/content/download/573877/9834690/Strat%C3%A9gie%20de%20l%27IA-UK_9%201%202020.pdf

Missão Permanente de Portugal junto da Organização do Tratado do Atlântico Norte. (2022a), Telegrama "DIANA – Definição do 'initial footprint" [n.º 341, de 4 de abril de 2022]. Bruxelas: Autor.

Missão Permanente de Portugal junto da Organização do Tratado do Atlântico Norte. (2022b), Telegrama "DIANA – Definição do 'initial footprint" [n.º 342, de 4 de abril de 2022]. Bruxelas: Autor.

Moor, J. (2006). The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years. AI *Magazine, 27*(4), 87-91. Retirado de https://aaai.org/ojs/index.php/aimagazine/article/view/1911/1809

Ng, A. (2017). Andrew Ng: Why AI Is the New Electricity [Online]. Retirado de https://www.gsb.stanford.edu/insights/andrew-ng-why-ai-new-electricity

North Atlantic Treaty Organization. (2021a). NATO 2030 – Factsheet [Online]. Retirado de https://www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/2106- factsheet-nato2030-en.pdf

North Atlantic Treaty Organization (2021b). Summary of the NATO Artificial Intelligence Strategy [Online]. Retirado de https://www.nato.int/cps/en/natohq/official_texts_187617.htm

North Atlantic Treaty Organization. (2022a). Initial DIANA Footprint [Online]. Retirado de https://www.nato.int/nato_static_fl2014/assets/pdf/2022/4/pdf/220407- DIANA-maps.pdf

North Atlantic Treaty Organization. (2022b). NATO sharpens technological edge with innovation initiatives [Online].Retiradode https://www.nato.int/cps/en/natohq/news_194587.htm

North Atlantic Treaty Organization Science & Technology Organization. (2019). *Science & Technology Trends: 2020-2040*. Retirado de https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf

North Atlantic Treaty Organization Standardization Office. (2019). *AJP-3 Allied Joint Doctrine for the Conduct of Operations*. Retirado de https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/797323/doctrine_nato_conduct_of_ops_ajp_3.pdf

North Atlantic Treaty Organization Standardization Office. (2020). *AAP-06 NATO Glossary of Terms and Definitions (English and French)*. Retirado de https://nso.nato.int/nso/nsdd/main/standards?search=Glossary

Oliveira, A. (2017). *Mentes Digitais: A Ciência Redefinindo a Humanidade* (3.ª Ed.). Lisboa: IST Press.

Parcelas, H. (2019). A Sexta Geração dos Conflitos - A Inteligência Artificial Autónoma na Guerra. Em: L. Saraiva, R. Vieira & J. Correia (Coords.) (2019). *Estudos Estratégicos das Crises e dos Conflitos Armados,* (207–227). Coleção "ARES", 29. Lisboa: Instituto Universitário Militar.

Rego, A., Cunha, M. P. E., & Meyer Jr, V. (2018). Quantos participantes são necessários para um estudo qualitativo? Linhas práticas de orientação. *Revista de Gestão dos Países de Língua Portuguesa, 17*(2), 43-57. Retirado de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1645-44642018000200004&lng=pt&tlng=pt

Santos, L. A. B., & Lima, J. M. M. V. (Coords.). (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação* (2.ª Ed, revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Sharre, P. (2018). *Army of none: autonomous weapons and the future of war*. New York: W. W. Norton & Company.

Stanford Institute for Human-Centered Artificial Intelligence. (s. d.). Global AI Vibrancy Tool: Who's leading the global AI race? [Página *online*]. Retirado de https://aiindex.stanford.edu/vibrancy/

Tarraf D. C., Shelton W., Parker E., Alkire B., Gehlhaus D., Grana J., Warren, K. (2019). *The Department of Defense Posture for Artificial Intelligence: Assessment and Recommendations*. Retirado de https://www.rand.org/content/dam

/rand/pubs/research_reports/RR4200/RR4229/R AND_RR4229.pdf

Tortoise. (s.d.). The Global AI Index [Online]. Retirado de https://www.tortoisemedia.com/intelligence/global-ai/

Villani, C. (2018). *For a Meaningful Artificial Intelligence - Towards a french and european strategy* [Estratégia Nacional de França para a IA]. Retirado de https://www.aiforhumanity.fr/pdfs/MissionVillani_Report_ENG-VF.pdf

Visual Paradigm. (s.d.). TOWS Analysis: A Comprehensive Guide [Online]. Retirado de https://online.visual-paradigm.com/knowledge/strategic-analysis/tows-analysis-guide/

ESTUDO 3 – O PAPEL DAS TECNOLOGIAS DE INTELIGÊNCIA ARTIFICIAL NA ADAPTAÇÃO DAS CAPACIDADES MILITARES ÀS AMEAÇAS MODERNAS – CONTRIBUTOS PARA O SEU EMPREGO[1]

THE ROLE OF ARTIFICIAL INTELLIGENCE TECHNOLOGIES IN ADAPTING MILITARY CAPABILITIES TO MODERN THREATS - CONTRIBUTIONS TO THEIR USE

Bruno Aguiar Couto
Major de Infantaria

Hugo Miguel Mansinho Barrote Rodrigues
Major de Infantaria

RESUMO

Este estudo foca-se nos potenciais contributos que a Inteligência Artificial pode oferecer para otimizar o Processo de Planeamento de Operações NATO no seio das Operações Especiais ao nível da componente. Emprega uma metodologia qualitativa, a pesquisa inclui análise documental e entrevistas semiestruturadas. Os resultados indicam vários desafios no Processo de Planeamento, incluindo a integração e análise de elevado volume de dados disperso em várias fontes, escassez de recursos e restrições de tempo. As tecnologias de Inteligência Artificial, particularmente *Machine Learning*, oferecem vantagens significativas automatizando tarefas analíticas complexas e integrando múltiplas fontes de dados, reduzindo assim o tempo e o pessoal necessário. O potencial da Inteligência Artificial para transformar operações militares é evidente na sua capacidade de fornecer análises em tempo real, criação de cenários preditivos e apoio à decisão. O estudo conclui que a implementação da Inteligência Artificial em determinados passos do processo de planeamento de operações, pode melhorar significativamente a eficiência.

Palavras-chave: Inteligência Artificial, *Machine Learning*, Processo de Planeamento de Operações, Operações Especiais, Otimização

[1] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto (CEMC 2023-2024). A versão integral encontra-se disponível nos no Centro de Recursos do Conhecimento do Instituto Universitário Militar.

ABSTRACT

This study focuses on the potential contributions that Artificial Intelligence can offer to optimize the NATO Operations Planning Process within the realm of Special Operations at the component level. Employing a qualitative methodology, the research includes document analysis and semi-structured interviews. The results highlight several challenges in the Planning Process, including the integration and analysis of large volumes of data dispersed across various sources, a scarcity of resources, and time constraints. Artificial intelligence technologies, particularly Machine Learning, offer significant advantages by automating complex analytical tasks and integrating multiple data sources, thereby reducing the necessary time and personnel. The potential of Artificial Intelligence to transform military operations is evident in its ability to provide real-time analyses, predictive scenario generation, and decision support. The study concludes that implementing Artificial Intelligence at certain stages of the operations planning process can significantly enhance efficiency.

Keywords: *Artificial Intelligence; Machine Learning; Operations Planning Process; Special Operations; Optimization.*

1. INTRODUÇÃO

O impacto das tecnologias na sociedade e nas operações militares, é hoje um facto que não pode ser ignorado. Com a sua evolução, as ameaças à segurança tornam-se cada vez mais complexas e interconectáveis, ultrapassando as fronteiras físicas. A transformação digital tornou-se uma questão de importância estratégica no campo da defesa e da segurança do ciberespaço para os diversos atores, tendo sido exemplo destes ataques, vários órgãos europeus e países da Aliança Atlântica (Comissão Europeia, 2020).

Com o emprego de Inteligência Artificial (IA) em larga escala no decorrer da invasão da Rússia à Ucrânia, desde fevereiro de 2022, o papel da IA atraiu a atenção da comunidade internacional e a de empresas tecnológicas, que procuram desenvolver e aprimorar continuamente esta tecnologia em prol da sua utilização no domínio militar (Konaev, 2023). A aplicação de IA, neste conflito tem vindo a ser empregue em Sistemas Aéreos Não Tripulados (SANT), em tarefas de *Intelligence, Surveillance and Reconnaissance* (ISR), à destruição de alvos com recurso a *loitering*

munition[2] e à sua aplicação em *softwares* com vista ao processamento e análise de grandes volumes de dados do campo de batalha (Fontes & Kamminga, 2023).

Na sequência da integração de IA na frente de batalha, o *Joint Special Operations University* (JSOU) identificou como necessidade de investigação o emprego de IA em prol das Operações Especiais (OEsp) de forma responsável (Simeral et al., 2022, p. 27).

Por sua vez, a *North Atlantic Treaty Organization* (NATO) identifica no seu conceito estratégico a importância estratégica das tecnologias emergentes e disruptivas, e a sua capacidade para influenciar o sucesso no campo de batalha (Strategic Concept, 2022, p. 5).

A nível nacional esta perspetiva é igualmente acompanhada sendo visível no Conceito de Estratégico de Defesa Nacional (2013, p. 45) a sua relevância refletindo-se nos vetores e linhas de ação estratégicas designadamente "valorizar os recursos e as oportunidades nacionais", incentivando à investigação, desenvolvimento e à inovação como essencial para elevar o nível tecnológico no sector da defesa.

Neste seguimento, a Diretiva Estratégica do Estado-Maior-General das Forças Armadas (Estado-Maior General das Forças Armadas [EMGFA], 2023, p. 26) reflete na linha de ação 2, do objetivo estratégico número 5 a necessidade de "promover a transformação digital": que visa analisar e avaliar os processos existentes, bem como desenvolver e implementar soluções digitais de melhoria da eficiência e da eficácia das atividades desenvolvidas pelas Forças Armadas (FFAA).

Focando o âmbito das OEsp a Diretiva Estratégica Setorial para as OEsp nas FFAA (EMGFA, 2022, p. 10) define como objetivo estratégico setorial número 9 – Explorar tecnologias emergentes para as OEsp, que implica impulsionar a inovação e a atualização tecnológica. Dado que o emprego deste tipo de forças ocorre em cenários altamente complexos, onde a informação a ser analisada é intrincada e o tempo de resposta é frequentemente reduzido existe a necessidade de otimizar o *Special Operations Component Command – Planning Process* (SOCC-P2).

Assim, este trabalho de investigação procura continuar, em certa medida, a investigação de Bettencourt, realizada no âmbito do Curso de Promoção a Oficial General sobre *Aplicação das tecnologias de inteligência artificial em operações militares* (Bettencourt, 2022), com enfoque na adaptação da capacidade militar relativamente ao Comando e Controlo (C2) frente às ameaças modernas.

[2] Sistemas de armas híbridos com características de mísseis e SANT (Breiner & Ferran, 2024)

Concomitantemente, como contributo para o cumprimento dos objetivos política e militarmente estabelecidos, urge fomentar o desenvolvimento de tecnologias emergentes e integrar a IA para potenciar as capacidades militares.

O objetivo geral (OG) desta investigação é propor contributos de como a IA pode otimizar o SOCC-P2. Para dar cumprimento ao OG, foram expressos dois objetivos específicos (OE): **OE1.** Identificar as principais dificuldades na aplicação do SOCC-P2; **OE2.** Analisar as capacidades da IA com aplicação no SOCC-P2. Após identificação do OG e OE, e por forma a dar resposta à resolução do problema enquanto pilar central da investigação, formulou-se a questão central (QC) e as respetivas questões derivadas (QD) (Santos et al., 2019, p. 49). Assim a **QC** concretiza: Como é que a IA pode otimizar o SOCC-P2?

Além da introdução, este trabalho estrutura-se em mais três capítulos culminando posteriormente nas conclusões. Assim, o segundo reporta-se ao enquadramento teórico e conceptual, expondo ainda o estado da arte; no terceiro descreve-se a metodologia e método conduzidos durante a investigação; no quarto apresentam-se os resultados sustentados nas entrevistas visando responder as QD e QC. Por último, nas conclusões avaliam-se os resultados obtidos, apresentam-se os contributos para o conhecimento e propõem-se recomendações de ordem prática.

2. ENQUADRAMENTO TEÓRICO E CONCEPTUAL

Este capítulo explora a revolução provocada pela IA no domínio militar, destacando o impacto transformador nas operações e no processo de planeamento militar contemporâneo. Através de uma análise detalhada do papel da IA no conflito Rússia – Ucrânia, bem como nas iniciativas e abordagens adotadas pela União Europeia e pela NATO, vislumbra-se uma perspetiva abrangente sobre como esta tecnologia está a redefinir as capacidades militares. Além disso, os desafios e oportunidades associados à integração da IA, enfatizam a necessidade de um equilíbrio entre inovação tecnológica e considerações éticas. Este enquadramento serve de base para compreender a crescente importância da IA na defesa e as implicações para o futuro das operações militares e da segurança global.

Adicionalmente, são expostos um conjunto de conceitos estruturantes que abarcam e contextualizam a investigação, bem como encorpam o modelo de análise.

2.1. Estado da arte

2.1.1. Inteligência Artificial no conflito Rússia – Ucrânia

O papel da IA no conflito entre a Ucrânia e a Rússia despertou a atenção dos meios de comunicação social, da NATO e empresas tecnológicas com vista a atualizar continuamente esta tecnologia em prol da sua utilização no domínio militar. A IA é uma tecnologia relativamente recente com poucas utilizações no campo de batalha anteriores à guerra da Ucrânia. No entanto é difícil avaliar que tipo de IA e tecnologias autónomas estão a ser empregues em tarefas e missões classificadas, e com que efeito pretendido, devido ao sigilo dessas missões (Konaev, 2023).

Por outro lado, é percetível que a IA desempenha um papel cada vez mais relevante na análise e no apoio à decisão, quer através do reconhecimento de alvos por imagens de satélite, quer pela análise de grandes volumes de dados geradores de informações de elevado valor estratégico e tático, no campo de batalha (Fontes & Kamminga, 2023).

No decorrer do conflito, as forças ucranianas têm empregado a IA na análise e cruzamento de grande volume de dados permitindo uma compreensão do campo de batalha mais clara e em tempo real, possibilitando a localização e identificação de possíveis alvos a serem abatidos, ou seja, contribuindo para o ciclo de *targeting*. Paralelamente, uma melhor compreensão do campo de batalha favorece uma tomada de decisão mais rápida e consciente (Dastin, 2023).

Uma das grandes inovações com impacto no conflito, tem sido o emprego da *MetaConstellation*. Esta ferramenta é uma rede de satélites que capta dados do campo de batalha, através de sensores e, com a IA analisa os dados para identificar posições inimigas, propor o meio mais eficaz a empregar na destruição do alvo e por último efetuar o *Battle Damage Assessment*[3], para melhorar a sua confiabilidade e precisão desta ferramenta (Dastin, 2023). Outra ferramenta alicerçada em IA utilizada no confronto é a *Clearview AI*, com vista a identificar soldados e espiões russos. A grande parte de identificação dos militares russos tem sido para notificar as famílias dos óbitos e dar a conhecer a realidade da frente de batalha à população russa. No entanto, esta ferramenta pode ser facilmente adaptada para identificação de alvos com vista à sua captura ou eliminação (Konaev, 2023, p. 13).

[3] Visa avaliar dos danos e efeitos infletidos num alvo quer na dimensão física, cognitiva e virtual (North Atlantic Treaty Organization [NATO]), 2021, pp. 5–2).

Outras gigantes tecnológicas como a Microsoft têm participado neste conflito com aplicação de IA em programas focados na proteção de infraestruturas contra ciberataques, *malwares*[4] destrutivos e *phishing*[5]. Além disso, tem participado na defesa contra a desinformação e propaganda (Watts, 2022).

Em suma, uma das principais lições que se tornou premente na guerra da Ucrânia é a necessidade de um grande investimento em capacidades para garantir um sistema de C2 rápido e eficiente, capaz de gerir vastas quantidades de dados e informações que possibilitem rápidas avaliações e reações aos movimentos do adversário, e assim garantir uma vantagem estratégica (Bauer, 2023, p. 15).

2.1.2. Inteligência Artificial na União Europeia

Até recentemente os exércitos europeus assentavam o seu planeamento de capacidades a longo prazo na obtenção de resultados relativamente fixos e previsíveis. Com as novas tecnologias civis e as suas potenciais aplicações na última década a evoluírem a uma velocidade impressionante, as FFAA viram-se obrigadas a incorporar a "resiliência inovadora" nos seus sistemas, o que exige capacidades ágeis com aptidão para absorver novas tecnologias ao longo do seu ciclo de vida, evitando assim a obsolescência ou a desativação antecipada dos sistemas (European Defence Agency [EDA], 2021, p. 6).

Em suma, nenhuma outra tecnologia de defesa emergente tem tido implicações tão abrangentes para operações militares quanto a IA, que se inicia com a capacidade dos algoritmos em fazer escolhas ótimas ou quase ótimas para alcançar objetivos específicos (EDA, 2021, p. 7).

Assim a União Europeia tem demonstrado um forte compromisso com a integração da IA na defesa, visando melhorar a eficiência, a segurança e a inovação nos sistemas de defesa europeus. Esta abordagem multifacetada tem incluído desde o desenvolvimento de tecnologias avançadas, à promoção de colaborações internacionais e à criação de leis reguladoras. Exemplo disso, são alguns dos projetos sob a égide da *European Defence Fund*. Um desses projetos desenvolvido pela EDA, iniciado em 2019 e com foco no apoio ao processo de tomada de decisão denomina-se *Clould Intelligence for Decision Making Support and Analysis*

[4] Qualquer programa ou arquivo intencionalmente prejudicial para um computador, rede ou servidor (Lutkevich, 2016).
[5] Prática fraudulenta realizada no ciberespaço por um atacante disfarçado de entidade confiável (Gillis, 2016).

(CLAUDIA), cujo objetivo é desenvolver uma ferramenta operacional capaz de gerir e processar a recolha de informações através de diversas fontes, desde a recolha de dados em fontes abertas até à recolha de informações classificadas, com o fim de rastrear ameaças híbridas e apoiar a tomada de decisão (EDA, 2021, p. 11).

2.1.3. Inteligência Artificial na NATO

O *Allied Command Transformation* da NATO perante múltiplos desafios globais e com as fronteiras entre a paz e a guerra cada vez mais difusas, explora a viabilidade de emprego de ferramentas tecnológicas, como a IA, para apoio à decisão de nível político- militar pretende-se com estas novas ferramentas refinar a análise de dados, aprimorar a consciência situacional estratégica e desenvolver análises preditivas, permitindo a criação e teste de várias ações potenciais para informar decisões em tempo real, mantendo a NATO preparada e proativa diante de potenciais crises (Giordano, 2023). Contudo, ainda não se verifica documentação que comprove a aplicação efetiva de IA nesse contexto, no seio da NATO.

2.1.4. Inteligência Artificial e o Processo de Planeamento militar

Num mundo onde a tecnologia evolui a passos largos, a IA tem-se destacado como uma tecnologia emergente nos mais diversos campos incluindo o militar. Segundo Branch (2018), a IA poderá revolucionar o processo de planeamento militar do nível operacional colocando um olhar crítico sobre as práticas atualmente desenvolvidas. O processo de tomada de decisão militar é uma metodologia sólida, mas que não tem alterado drasticamente nas últimas décadas, ao contrário do atual ambiente operacional cada vez mais volátil, incerto, complexo e ambíguo.

Destarte, com a integração da IA, será possível processar e analisar elevados volumes de dados de informações de forma mais rápida do que pelos tradicionais métodos humanos, possibilitando compreensões mais profundas e previsões precisas nas tomadas de decisão. Poderão também auxiliar na identificação de padrões, tendências ou anomalias menos óbvias ao olho humano o que poderão ser um forte contributo para o processo de planeamento. A IA surge também como uma possibilidade para simular cenários operacionais complexos, possibilitando aos planeadores dos Estados-maiores identificar e explorar diferentes modalidades de ação e testá-las sem riscos associados no mundo real. Por último, Branch (2018) visualiza que a IA pode mitigar os vieses cognitivos desenvolvidos naturalmente pelo homem, durante o processo planeamento e tomada de decisão (Branch, 2018).

Já Grady (2023, pp. 16–17) refere que a IA é tida como um elemento-chave na modernização das FFAA americanas, especialmente em termos de integração e de C2, com o objetivo de garantir uma vantagem necessária para mitigar e derrotar ameaças militares *peer to peer*[6].

Pese embora, a chave para integração e implementação de IA no instrumento militar, especialmente no que concerne ao C2 e tomada de decisão, reside na necessidade de balancear entre a autonomia das máquinas (velocidade e eficácia) e o controlo que o homem detém. O desafio é encontrar um equilíbrio onde a IA pode ser empregue para acelerar o processo de planeamento e, por sua vez, a tomada de decisão, sem sacrificar a supervisão e o julgamento humano necessário para garantir a tomada de decisões éticas e precisas. Paralelamente, a integração de IA nos exércitos não exige apenas a adoção de novas tecnologias, mas também de um corpo especializado que abrange desde o entendimento técnico de IA às implicações éticas e estratégicas do seu emprego (Pfaff et al., 2023, p. 28).

Não obstante, o estudo de caso elaborado pela RAND *Corporation* acerca do conflito na Ucrânia, demonstra como a análise de dados baseada em IA forneceu aos seus comandantes novas perceções do ambiente operacional, o que corrobora a sua aplicação e colaboração com humanos, como parte de um sistema de tomada de decisão com vista a aprimorar a eficácia das operações militares. Destaca-se ainda, a potencialidade da IA em apoiar de forma efetiva o processo de tomada de decisão, que é tanto mais eficiente quando emparelhada com analistas de informação humanos, com um vasto entendimento sobre o problema em questão (Robinson et al., 2023).

Por sua vez, Kim (2023, pp. 6-9) vislumbra a integração da IA como ferramenta de orquestração das capacidades militares, explorando o sacrifício e deceção, tal como num tabuleiro de xadrez, em prol das operações Multidomínio. No entanto, o desenvolvimento de algoritmos de IA para uso militar deve estar consorciado com medidas de eficácia, pois a avaliação de um algoritmo deve ser efetuada pelo impacto do seu trabalho na missão e não apenas na deteção de alguns fatores ou dados, ou seja, garantir que essa tecnologia contribui de maneira significativa para objetivos operacionais e estratégicos para o qual foi desenhada.

[6] Confronto entre duas nações ou entidades que possuem capacidades militares semelhantes.

2.1.5. Ameaças Modernas

Enquadrado pelo conceito estratégico da NATO (2022) pode-se afirmar que as ameaças modernas contra a Aliança e Portugal provêm da Federação Russa, através da violação das normas e princípios que contribuem para a estabilidade e segurança da Europa. Violação esta refletida através do emprego de táticas híbridas convencionais e cibernéticas, campanhas de desinformação, instrumentalização da migração, manipulação do fornecimento energético e emprego de medidas económicas coercivas. Outras ameaças modernas definidas, são o terrorismo e a instabilidade em África e no Médio Oriente. A República Popular da China é também reconhecida como ameaça devido ao recurso a políticas e economias coercivas com vista a aumentar a sua influência global, assim como pelas operações híbridas e cibernéticas maliciosas desenvolvidas contra os Aliados (NATO, 2022, pp. 3 e 4).

A proliferação de armas nucleares e químicas, e o seu possível emprego por atores estatais continua a ser uma preocupação constante (NATO, 2022, p. 5).

O ciberespaço é palco de muitos atores com intensões maliciosas, por isso, as tecnologias emergentes e disruptivas para além de trazerem oportunidades também originam riscos. Estas tecnologias revelam-se assim de elevada importância estratégica alterando as dinâmicas dos conflitos (NATO, 2022, p. 5).

2.1.6. Síntese conclusiva

A IA tem emergido como uma força transformadora nas operações militares e estratégias de defesa, particularmente evidenciada no conflito Rússia – Ucrânia. A sua capacidade de processar e analisar informações rapidamente oferece perceções estratégicas e táticas, melhorando a eficiência e eficácia das operações militares. Este facto ergueu iniciativas globais que visam integrar a IA como um pilar central na modernização da defesa e na promoção de uma segurança coletiva mais robusta.

No entanto, a integração da IA no domínio militar traz consigo desafios significativos, destacando-se a necessidade de equilibrar a autonomia das máquinas com o controlo humano para garantir decisões éticas e precisas. A colaboração entre humanos e IA, especialmente na tomada de decisões e no planeamento militar, é crucial para explorar plenamente o potencial desta tecnologia, sem sacrificar a supervisão humana indispensável. A evolução da IA na defesa representa uma oportunidade sem precedentes para avançar nas capacidades militares contudo, exige uma abordagem cuidadosa que priorize a ética, a responsabilidade e a sustentabilidade a longo prazo, para fazer face às ameaças modernas.

Mediante o exposto torna-se pertinente e de relevância atual estudar o impacto da IA no PPO e como pode otimizar o SOCC-P2 atual.

2.2. Base conceptual

Para uma melhor perceção da presente investigação importa definir um conjunto de conceitos estruturantes que sustentam o estudo e adicionalmente norteiam o tema em apreço, abaixo desenvolvidos.

2.2.1. Inteligência Artificial

Na atualidade, verifica-se que a IA encontra-se em todos os setores públicos e privados, não sendo a exceção o domínio militar. Neste contexto, a IA é definida como um campo específico da ciência da computação que explora como é que as funções de computação automatizadas podem assemelhar-se às funções dos seres humanos (Grzegorzewski, 2021).

Desta forma a IA é entendida como a simulação de processos de inteligência humana por máquinas, especialmente sistemas computacionais. De forma genérica, o funcionamento da IA resume-se à recolha de grandes quantidades de dados, ao processamento dos mesmos e procura de correlações e padrões com vista a efetuar previsões. A sua programação baseia-se em quatro habilidades cognitivas sendo a aprendizagem, a autocorreção, o raciocínio e a criatividade (Laskowski, 2023).

Embora possa ser classificada de diversas formas, dependendo dos critérios utilizados, para este estudo a IA vai ser agrupada por nível de capacidade, existindo três categorias. A Inteligência Artificial Estreita (ANI) foca-se em realizar tarefas específicas, dentro de um conjunto limitado de parâmetros e controlos, sendo nesse sentido, limitada a executar apenas as tarefas previstas na sua programação, ainda que de forma bastante eficaz, sendo exemplo disso os assistentes virtuais e os carros autónomos (Hashemi-Pour, 2023).

A Inteligência Artificial Geral (AGI), representa uma máquina com a capacidade de entender, aprender e aplicar a sua inteligência numa vasta gama de tarefas de forma semelhante à inteligência humana. No entanto, a AGI ainda é um objetivo a longo prazo na pesquisa mantendo-se apenas como uma teoria (Hashemi-Pour, 2023).

A Inteligência Artificial Superinteligente (ASI), é um conceito ainda mais avançado e teórico, onde a IA para além de replicar a inteligência humana consegue superá-la, obtendo uma capacidade de raciocínio e resolução de problemas

ultrapassa a mente humana. No entanto, esta tecnologia ainda não se vislumbra num futuro próximo (Grzegorzewski, 2021). Para além destas categorias, existem ainda subcampos da IA constantes na figura 1 importantes de serem identificados e conceptualizados pela especificidade de cada um e pelo modo como podem ser empregues em prol do domínio militar.

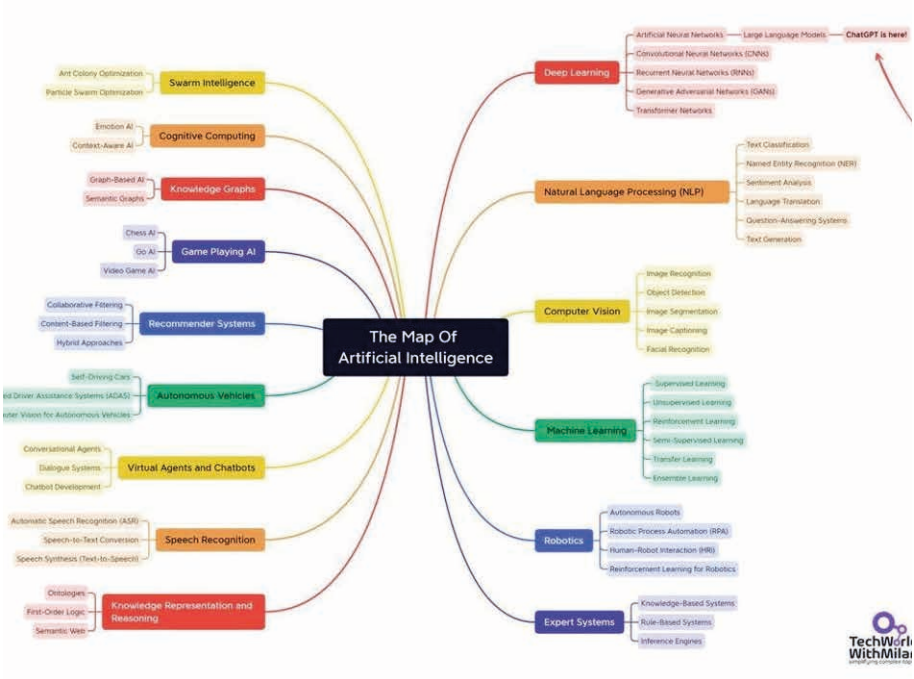

Figura 1 – Diagrama representativo dos subcampos da IA
Fonte: Milanović (2023).

2.2.1.1. *Machine Learning*

O *Machine Learning* (ML) concentra-se na aprendizagem de computadores através de processos interativos como interpretar dados e aprender com os mesmos, ou seja, permite que os computadores aprendam a realizar tarefas sem serem explicitamente programados para isso. Com o ML os algoritmos são treinados para identificar padrões e fazer previsões ou até tomar decisões com base nos dados fornecidos, no entanto, dependem mais da intervenção humana

para aprender. É utilizado já em diversas aplicações, desde compras online, carros autónomos, diagnósticos médicos e sistemas financeiros (Tucci, 2023).

Em alguns casos os algoritmos são sobrepostos com vista a criar redes neurais mais intrincadas, permitindo desta forma elaborar tarefas cada vez mais complexas e diferenciadas associando o conceito de *Deep Learning* (DL), que na verdade se constitui como um subcampo do ML. A grande diferença encontra-se na forma como cada algoritmo aprende (International Business Machines Corporation [IBM], 2021).

2.2.1.2. *Deep Learning*

O DL tenta replicar os neurónios e sinapses do cérebro humano através de uma rede neural, que consiste numa rede de nós interconectados com dados processados em diversas camadas. Assim sendo, o DL é particularmente eficaz para o reconhecimento de padrões e tomadas de decisão com base em grandes volumes de dados sendo utilizado em diversas aplicações como processamento de linguagem natural, reconhecimento da fala, jogos e diagnósticos médicos (Gillis, 2023).

O DL e as redes neurais são reconhecidas por acelerar o progresso em áreas como a *Machine Vision* (MV) ou *Natural Language Processing* (NLP) que na prática trabalham ligadas ao DL (IBM, 2021).

2.2.1.3. *Natural Language Processing*

O NLP visa a integração entre os computadores e a linguagem humana, cujo objetivo é permitir que os computadores interpretem a linguagem humana de maneira útil incluindo tarefas como tradução automática, reconhecimento da fala e geração de texto (Lutkevich, 2023b).

2.2.1.4. *Expert System*

O *Expert System* (ES) é um sistema com capacidade de tomar decisão num campo específico tal como um especialista humano, tendo sido utilizados em diversas áreas específicas como a medicina no diagnóstico de doenças e sugestões de tratamento, na engenharia efetuando diagnósticos de falhas em máquinas, e finanças na análise de investimentos e deteção de fraude financeira (Lutkevich, 2023a).

2.2.1.5. *Machine Vision*

A MV é a interpretação de imagens do mundo real para permitir que as máquinas possam realizar tarefas complexas como identificação, inspeção e rastreamento de objetos. O MV pode ser utilizado em reconhecimento de padrões para leitura de matrículas ou códigos de barras, em robótica com vista a orientar robôs e ainda segurança e vigilância com vista à deteção de atividades suspeitas (Yasar, 2023).

2.2.2. Operações Especiais

De acordo com a doutrina da NATO, as OEsp são atividades militares conduzidas por pessoal especialmente selecionado, organizado, treinado e equipado que usam técnicas e modo de emprego distintos. São tidas como uma capacidade militar empregue para apoiar a NATO a alcançar objetivos de nível estratégicos e operacional. As OEsp podem ser conduzidas em todo o espetro das operações militares, de forma independente ou com forças convencionais. As OEsp diferem de outras forças principalmente pelas suas capacidades distintas, agilidade e flexibilidade, não sendo um substituto das forças convencionais. O comando das OEsp é exercido através de um Comando de Componente de Operações Especiais, geralmente debaixo de um quartel-general de nível operacional ao mesmo nível das restantes componentes terrestres, aérea e marítima (NATO Special Operations Headquarters, 2014, p. 11 e 12)

A nível nacional as OEsp são também reconhecidas como uma capacidade militar conjunta (EMGFA, 2022).

2.2.3. Processo de Planeamento de Operações

O PPO é uma ferramenta cuja finalidade é a de desenvolver planos de operações adequadamente detalhados, que abordem todos os fatores relevantes para a condução eficiente e bem-sucedida de uma operação. O PPO a nível da NATO descreve como a Aliança inicia, desenvolve, coordena, aprova, executa e cancela planos de operações. Desta forma, o PPO é aplicado transversalmente nas atividades de planeamento, de forma colaborativa pelos níveis estratégico, operacional e adaptado ao nível da componente tática (Allied Command Operations Comprehensive Operations Planning Directive, Version 3.1 [COPD V3.1], 2023, pp. 1–1).

2.2.4. *Special Operation Command Component – Planning Process*

Após a criação do *Special Operations Component Command* (SOCC) ao nível NATO a COPD foi também ajustada para o SOCC-P2 por este comando, para conduzir de forma eficiente o planeamento colaborativo com o escalão operacional conforme apresentado na figura 2 (NATO, 2019, pp. 1-2).

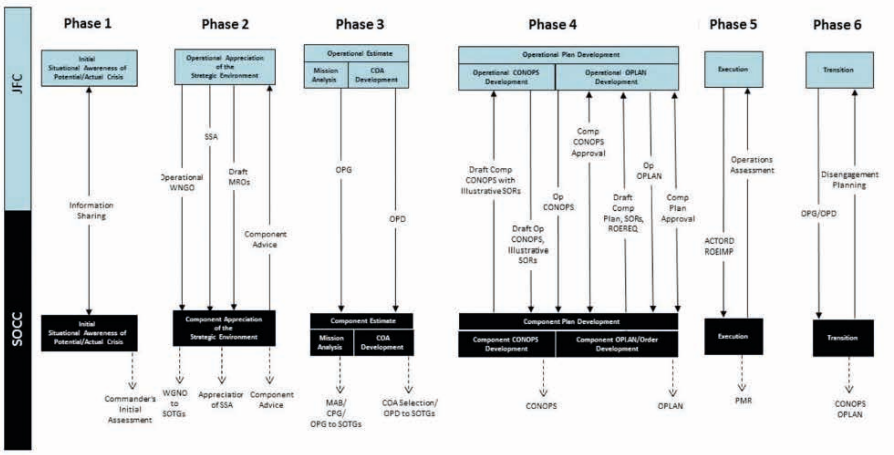

Figura 2 – Interação entre o SOCC e o JFC durante o SOCC-P2
Fonte: Adaptado a partir de NATO (2019, pp. 1-2).

No âmbito desta investigação a lupa é colocada sobre a fase 3 *Estimate* ao nível do SOCC onde é elaborada a análise da missão e o desenvolvimento das modalidades de ação, para posteriormente dar continuidade a fase seguinte do processo de planeamento.

2.3. Modelo de análise

Com a exposição do estado da arte verifica-se que existem condições para desenvolver a investigação, não só por acrescentar valor para as FFAA e em particular para as OEsp, mas também pela pertinência que representa para a consecução dos objetivos estratégicos definidos na Diretiva Estratégica Setorial para as OEsp. Neste seguimento, elaborou-se um modelo de análise (Quadro 1), através do qual se estruturou e sistematizou os objetivos, as questões, conceitos, dimensões e respetivas técnicas de recolha de dados.

Quadro 1 – Modelo de análise

Objetivo Geral (OG)	Propor contributos de como a IA pode otimizar o SOCC-P2			
Questão Central (QC)	Como é que a IA pode otimizar o SOCC-P2?			
Objetivos Específicos	**Questões Derivadas**	**Conceitos**	**Dimensões**	**Técnicas de Recolha**
OE1: Identificar as principais dificuldades na aplicação do SOCC-P2.	**QD 1:** Quais as principais dificuldades na aplicação do SOCC-P2?	• PPO NATO • SOCC- P2	• Ferramentas da fase 3 do SOCC-P2 • Processos da fase 3 do SOCC-P2	• Análise documental • Entrevistas semiestruturadas
OE2: Analisar as capacidades da IA com aplicação no SOCC-P2.	**QD2:** Quais as capacidades da AI com aplicação no SOCC-P2?	• IA	• Análise de informações • Processo de planeamento • Redução de tempo • Simulação de cenários	• Análise documental • Entrevistas semiestruturadas

3. METODOLOGIA E MÉTODO

O racional que se pretende seguir nesta investigação irá procurar verificar o que já existe a nível da IA em outras áreas de investigação passível de ser aplicado ao PPO NATO mais concretamente no SOCC-P2, com a finalidade de propor contributos da sua aplicação no SOCC-P2 com vista à sua otimização.

Metodologicamente, consoante os ensinamentos de Santos et al. (2019, p. 19), esta investigação pretende seguir um raciocínio do tipo indutivo, uma vez que se irá observar as aplicações de IA em contextos similares e a partir desta desenvolver propostas sobre como a IA pode ser aplicada no planeamento de operações. Segue uma estratégia de investigação qualitativa, inicialmente, através da análise documental de artigos científicos relacionados com aplicação de IA e doutrina relativa ao planeamento de operações e num segundo momento, com a realização de entrevistas semiestruturadas a elementos da CPOE[7] e da NATO que apliquem o SOCC-P2, com vista a identificar as principais dificuldades e dar resposta a QD1. Seguidamente, através da análise documental e entrevistas semiestruturadas a entidades especializadas em trabalhar IA analisar-se-á o que existe em termos de IA passível de ser adaptado ao SOCC-P2, para dar resposta à QD2. O desenho de pesquisa aplicado baseia-se no estudo de caso, na medida em

[7] A CPOE constitui-se como o núcleo inicial do Comando de Componente de OEsp (Decreto-lei n. º19/2022, de 24 de janeiro) e organicamente no Comando Conjunto para as Operações Militares/ EMGFA na dependência do Comandante Operacional das Forças Armadas

que se pretende focar no evento contemporâneo da aplicação da IA no SOCC-P2 da CPOE (Yin, 2024).

No contexto da investigação, conforme Santos e Lima (2019, p. 33), o estudo de caso será temporalmente transversal, uma vez que o estudo examinará a situação atual da aplicação da IA no SOCC-P2 da CPOE, num momento específico no tempo. Ou seja, o estudo da IA terá como enfoque as condições atuais, práticas, desafios e oportunidades relevantes no contexto atual para otimização do SOCC-P2 da CPOE, balizado entre 2021 e março de 2024.

Para a coleta dos dados necessários a esta pesquisa, foram empregues técnicas típicas de estratégias qualitativas, incluindo análise documental e entrevistas (Santos & Lima 2019, p. 28). A pesquisa foi fundamentada na análise de fontes primárias, tais como documentos oficiais, diretivas, publicações doutrinárias e entrevistas semiestruturadas, utilizando um guião como ferramenta para este último método.

A investigação teve a colaboração de militares que desempenharam funções com participação ativa na condução do SOCC-P2, quer a nível nacional na CPOE, como ao nível da NATO no *Allied Special Operations Forces Command* (SOFCOM) e no *Allied Rapid Reaction Corps* (ARRC), além dos militares, participaram ainda na investigação especialistas de IA, que aglutinam experiência e conhecimento atual para sustentar a presente investigação (Rego et al., 2018, p. 52).

Para garantir a participação dos entrevistados, inicialmente foram realizados contatos diretos, seguidos do envio dos guiões de entrevista por email. Após obter o consentimento dos participantes para se envolverem no estudo, as respostas foram recolhidas através de três modalidades: presencialmente, email ou videoconferência.

Tabela 1 – Lista de entrevistados

Cargo/Função	Posto/título e Nome
Research professor for strategy the military profession and ethics at the Army War College, USA Integrating AI into the US Army's	Anthony Pfaff
Deputy and Branch Head of Futures Development Division in SOFCOM, Mons, Belgium	Tenente-coronel Giovanni Vuocolo
Chefe da Divisão de Planeamento de Forças do Estado-Maior do Exército	Tenente-coronel Gradíssimo de Oliveira
Quartel General do ARRC G35 Team Leader Equipa C (Professor do IUM da área de Ensino de Operações de fev21 a out21; Professor do IESM da área de ensino de operações de jul11 a set14)	Tenente-coronel Morais dos Santos

[Cont.]

Oficial de Planos da CPOE	Major António Lopes
Oficial de Operações da CPOE	Major Hugo Brigas
Docente e gestor de projetos, Autónoma Academy, Universi- dade Autónoma de Lisboa	João Paulo Feijoo
Investigador de IA e Professor no Instituto Superior de Engenharia do Porto	João Carneiro
Engenheira na Devoteam na área da IA	Rita Alves Ribeiro
Engenheiro Informático na Devoteam na área de IA	João Morgado
Mestrado em IA	Pedro Águas

Na fase exploratória, os instrumentos utilizados foram essencialmente a análise documental, como legislação, artigos científicos, diretivas, doutrina na área do planeamento NATO e das OEsp, alguns contactos exploratórios a especialistas ligados às OEsp, ao oficial de planos da CPOE e ainda a elementos interessados sobre a temática de IA.

Durante a fase de análise e conclusão, além de prosseguir com a análise documental, utilizaram-se entrevistas como método de recolha de dados. Para isso, a entrevista versou dois grupos distintos entrevistados. Um dos grupos focais da entrevista inclui militares com vasta experiência na aplicação do SOCC-P2, com vista a recolher as principais dificuldades na condução deste processo de planeamento. Por outro lado, o segundo grupo entrevistado consistiu em civis especialistas na área da IA, com vista a entender que pontos fortes e vulnerabilidades tem a IA na sua possível aplicação em processo de planeamento e apoio à tomada de decisão. Cabe destacar dois entrevistados que responderam à totalidade da entrevista: Anthony Pfaff, Professor investigador de *Strategy the military profession and ethics* no Army War College Carlisle, Pensilvânia nos Estados Unidos da América, responsável também por integrar a IA no exército americano; e o Tenente-Coronel Vuocolo Giovanni, chefe da *Futures Development Division*, no SOFCOM em Mons na Bélgica.

No desenvolvimento da análise categorial das respostas dos participantes através da técnica de análise de conteúdo, identificaram-se unidades de contexto e estabeleceram-se unidades de registo correspondentes. Estas unidades de registo foram posteriormente organizadas em subcategorias, que foram agrupadas em categorias maiores (Sarmento, 2013, pp. 53-66). A análise foi subsequentemente conduzida com o objetivo de responder às QD e seguidamente à QC.

4. APRESENTAÇÃO DOS DADOS E DISCUSSÃO DOS RESULTADOS

No presente capítulo apresentam-se os dados resultantes da análise de conteúdo desenvolvida sobre as entrevistas semiestruturadas aos onze entrevistados (Sarmento, 2013, pp. 53-66). Procura-se nesta fase dar resposta às QD e, concomitantemente, discutir os resultados obtidos, com vista a dar resposta a QC.

Após a análise de conteúdo foram identificadas três grandes categorias que são abordados neste capítulo onde se inserem diversas subcategorias e demais unidades de registo.

4.1. Principais dificuldades na aplicação do SOCC-P2

A análise das entrevistas revela que são identificadas de forma comuns diversas dificuldades na condução do SOCC-P2. Uma subcategoria significativa é a "dificuldade de análise" que engloba desafios específicos enfrentados pelos militares em empregar esta ferramenta. Seguidamente são detalhados cada uma das unidades de registo (Tabela 2).

Tabela 2 – Dificuldades do SOCC-P2 relativas a dificuldades de análise

Dificuldade de análise	1.1.1 Complexidade das ferramentas
	1.1.2 Incorporação de diversas fontes
	1.1.3 Elevado volume de informação

A complexidade das ferramentas e tecnologias empregues durante a realização da fase 3 do SOCC-P2, conforme a B. Oliveira (entrevista por *email*, 09 de março de 2024) e H. Brigas (entrevista por *email*, 06 de março de 2024), representam um desafio para os militares especialmente para aqueles que não estejam familiarizados com essas mesmas ferramentas, sendo exemplo disso o diagrama de influências, a determinação dos Centros de Gravidades (CoG) até ao desenho de operações. Da mesma forma, A. Lopes (entrevista por *email*, 07 de março de 2024) refere que face à rápida transmissão de informações com efeitos imediatos aumentam a dificuldade de emprego destas ferramentas e correlação entre elas em temo oportuno.

Por sua vez, integrar e analisar informações disponíveis de diversas fontes, revela-se difícil. A análise holística a fim de obter um entendimento situacional

sobre toda a informação e dados disponíveis, vislumbra-se morosa e complexa, tanto quanto mais intrincados forem os cenários aos quais, por norma, as OEsp estão adstritas (A. Pfaff, entrevista por videoconferência, 22 de fevereiro de 2024).

Concomitantemente aliado à "incorporação de diversas fontes" está associado um elevado volume de informação que, por si só, representa uma dificuldade acrescida pela quantidade de dados a processar e analisar para construir uma *Common Operational Picture*[8] precisa do cenário complexo que se possa apresentar (A. Pfaff, *op. cit.*).

Outra das subcategorias identificadas relacionadas com a dificuldade do SOCC-P2 está estritamente relacionada com o fator humano, englobando desafios específicos elencados abaixo (Tabela 3).

Tabela 3 – Dificuldades do SOCC-P2 relativas ao fator humano

Fator Humano	1.2.1 Formação e Treino
	1.2.2 Falta de recursos humanos
	1.2.3 Coordenação e comunicação

"A falta de formação e de um treino adequado dos membros de um staff pode dificultar a utilização eficaz das ferramentas e técnicas disponíveis" (B. Oliveira, *op. cit.*), o que obriga o desenvolvimento de pessoal com formação técnica para a condução do SOCC-P2 e a respetiva manutenção dessa formação e treino para garantir a proficiência desses especialistas permitindo a diminuição do tempo despendido durante a análise e realização de tarefas específicas (M. Santos, entrevista por *email*, 08 de março de 2024).

Aliado a este fator, existe ainda a escassez de recursos humanos, um problema transversal às FFAA, que impõe uma sobrecarga aos militares com responsabilidades no planeamento de operações. Processo esse que, por si só, já representa um elevado consumo de tempo e de recursos humanos, desde a recolha, tratamento até à análise das informações. Esta falta de recursos humanos leva a que o tempo despendido seja maior para a uma correta e eficiente análise. Caso o tempo seja limitado origina a uma análise mais superficial podendo originar lapsos ou erros de análise (B. Oliveira, *op. cit.*).

[8] Refere-se a uma visão unificada e precisa da situação operacional num determinado momento.

Em estreita ligação com este fator, temos ainda a coordenação e comunicação entre os elementos de um Estado-maior sendo este crucial e desafiador especialmente em ambientes multinacionais onde a interação entre especialistas de diversos campos e matérias têm de interligar as suas diferentes perceções para retirar possíveis vieses de análise (G. Vuocolo entrevista por *email*, 12 de março de 2024). Assim, a partilha de informação durante o SOCC-P2 em ambiente multinacional, bem como, a uniformização das ferramentas e procedimentos a empregar ao nível de um Estado-maior do SOCC seja de extrema importância (H. Brigas, *op. cit.*).

Em paralelo ao fator humano, são identificados outros recursos intrinsecamente ligados como mais um desafio à condução do SOCC-P2, conforme Tabela 4.

Tabela 4 – Dificuldades do SOCC-P2 relativas aos recursos

Recursos	1.3.1 Falta de Tempo
	1.3.2 Sobreposição de tarefas

"Analisar e interpretar as informações para entender o ambiente operacional, as capacidades do inimigo e outras variáveis relevantes, pode consumir uma quantidade significativa de tempo" (B. Olveira, op. cit.) sendo que "o tempo disponível é determinante para a construção de um modelo correto de análise" (M. Santos, op. cit.). No entanto, quando o fluxo de informação é realmente sobrelevado, a capacidade humana de analisar toda a informação no tempo disponível revela-se insuficiente face à necessidade de respostas à velocidade da relevância, pelo que a seleção e avaliação da informação a analisar e dos recursos necessários para apoiar essa mesma análise é deveras importante face à restrição de tempo imposta. O que poderá originar lacunas de informação ou análises superficiais em determinados assuntos, podendo dar origem erros de interpretação da correta situação (A. Pfaff, *op. cit.*).

Nesse mesmo prisma, à falta de recursos humanos já acima elencada obriga à acumulação e a sobreposição de tarefas, originando muitas vezes a condução de processos de planeamento de forma empírica baseados no histórico já existente devido às restrições de tempo, face ao avolumado número de tarefas em mãos (A. Lopes, *op. cit.*).

Em suma, as principais dificuldades identificadas pelos entrevistados na condução da fase 3 do SOCC-P2 são: a integração e análise do elevado volume de informações disponíveis e presentes em diversas fontes; a falta de pessoal especializado para conduzir o processo de planeamento; escassez de recursos humanos; e condicionamentos de tempo. Este desiderato sustenta-se como resposta à QD1: Quais as principais dificuldades na aplicação do SOCC-P2? E consequentemente é atingido o OE1.

Portanto a atenção a estas áreas é crucial para otimizar o SOCC-P2, reforçando a eficácia operacional num ambiente cada vez mais complexo e volátil.

Da análise às entrevistas realizadas foi possível identificar duas categorias relacionadas com as capacidades da IA com aplicação na fase 3 do SOCC-P2. Por um lado, verificam-se as diversas vantagens e vulnerabilidades particulares da IA e, por outro lado, identificam-se potencialidades para aplicação de IA no SOCC-P2 que são lavrados abaixo.

4.2. Pontos fortes e vulnerabilidades da Inteligência Artificial

As diversas vantagens (Tabela 5) e vulnerabilidades particulares da IA são lavrados abaixo e encontram-se agrupadas em oito unidades de registo, distribuídas pelas duas subcategorias.

Tabela 5 – Vantagens da IA

Vantagens	2.1.1 Analisar informações incertas
	2.1.2 Relacionar e analisar
	2.1.3 Gestão de elevado número de dados em tempo real
	2.1.4 Capacidade para simulação
	2.1.5 Comunicação entre sistemasw

No que concerne às vantagens verifica-se que a IA, conforme J. Feijoo (entrevista por *email*, 28 de fevereiro de 2024) tem a capacidade para "lidar com informações contraditórias, filtrá-las e validá-las relacionando interactivamente com as fontes de informação no terreno e de outro modo detetar prováveis fraudes e intromissões". Por sua vez, J. Carneiro (entrevista por videoconferência, 05 de março de 2024) frisa a capacidade da IA para lidar com a incerteza e lógica difusa, e daí depreender qual a melhor solução adotar face as informações presentes.

Outras duas vantagens da IA, já refletidas por Bauer (2023, p. 15), encontram-se interligadas, sendo a capacidade de analisar e relacionar dados e informações em tempo real, "com caudais de informação muito para além do que as capacidades humanas alcançam" (J. Feijoo, *op. cit.*). Essa análise de informações não se limita apenas a documentos escritos, mas também à análise de fotografias, imagens, vídeos, padrões com vista a elaborar conclusões e predições. Não deixando de sinalizar conforme P. Águas (entrevista presencial, 26 de fevereiro de 2024) que "quantos mais dados a IA tiver para analisar maior performance terão os resultados", uma vez que será mais fácil aos algoritmos identificar padrões complexos, em contrapartida quantos mais dados o ser humano tiver para analisar, mais superficial será essa análise uma vez que os condicionamentos de tempo não lhe permitirão aprofundar essa análise.

Uma reconhecida capacidade da IA elencada pelos demais entrevistados converge com a visão de Branch (2018) que é a simulação e predição de cenários, consoante as variáveis ambientais e reações contrárias definidas pelos programadores com vista a projetar ou interpretar possíveis cenários estratégicos, táticos, ou mesmo a nível logístico na previsão, otimização e alocação de recursos (J. Feijoo, *op. cit.*).

Por último, a capacidade de colocar sistemas a comunicar com base em informações trocadas entre si, vem apoiar a tomada de decisão de forma mais célere, potenciando o funcionamento destes sistemas de forma proativa sem intervenção humana (J. Carneiro, *op. cit.*). Por outras palavras, a IA possibilita que a informação recolhida através de sensores na frente de batalha, quer através de ISR ou outro, seja enviado e analisado por outro sistema à retaguarda que o identifique como um alvo e, automaticamente designe um sistema de armas para bater esse mesmo alvo, conforme corroborado por Dastin (2023) no conflito entre a Rússia e a Ucrânia e sob a lupa do PPO torna-se pertinente no ciclo de *targeting* e na fase 5 do mesmo.

Em contrapartida, são expostas três grandes vulnerabilidades da IA que são tratadas abaixo, conforme Tabela 6:

Tabela 6 – Vulnerabilidades da IA

Vulnerabilidades	2.2.1 Vieses
	2.2.2 Limitações
	2.2.3 Ligação

A aplicação de IA na análise de informações elimina possíveis vieses humanos, em contrapartida, são introduzidos vieses pelos próprios algoritmos que podem distorcer e influenciar a qualidade final do produto (A. Pfaff, *op. cit.*). Estes vieses introduzidos podem surgir por situações utilizadas para treinar o algoritmo já enviesadas reproduzindo esse viés em futuras soluções ou quando o fluxo de informação ao qual o algoritmo tem acesso seja contaminado por informação manipulada ou corrompida (J. Feijoo, *op. cit.*).

No que concerne às limitações é possível adiantar que a IA é limitada à aprendizagem que lhe for fornecida (J. Feijoo, op. cit.). Por outro lado, outra grande limitação passa pela necessidade de colocar todos os dados devidamente estruturados e arrumados para que o algoritmo possa, de forma fiável, elaborar conclusões credíveis e otimizar opções (A. Pfaff, *op. cit.*).

Por conseguinte, a capacidade da IA é tanto, ou quanto maior se tiver ligação online ou se cingir a um sistema designado por *self-contain* a funcionar localmente sem uma ligação *online* (J. Carneiro, *op. cit.*). O facto de funcionar em sistema *online* poderá colocar questões de segurança em causa para além dos elevados custos necessários para manter uma *cloud* dedicada. Contudo, possibilita operar algoritmos mais pesados, com maior qualidade e maior acesso a informação possibilitando a comunicação entre sistemas para trabalhar em rede (A. Pfaff, *op. cit.*). Ainda assim, aplicação de IA *self-contain* em pequenas empresas para reduzir custos já é uma realidade, tendo como limitação o emprego de modelos de IA mais leves e com menos parâmetros (J. Carneiro, *op. cit.*).

4.3. Potencialidades para aplicação de Inteligência Artificial

As potencialidades para aplicação de IA enumeradas durante as entrevistas foram agrupadas segundo três subcategorias sendo elas: o processo de planeamento, o fluxo de informação e a aplicação por técnica de IA. Relativamente ao processo de planeamento, as unidades de registo associadas são as elencadas na Tabela 7.

Tabela 7 – Potencialidades para aplicação de IA no SOCC-P2

Processo de planeamento	3.1.1 Briefing Análise da Missão (BAM)
	3.1.2 *Course of Action* (CoA)

A aplicação de ferramentas e elaboração de produtos relacionados com o BAM apontados por H.Brigas (*op. cit.*) e corroborado pelos restantes militares entrevistados tais como: Entender o ambiente operacional e os principais atores e a ligação entre eles; Analisar e determinar todos os factos; Centros de Gravidade (CoG); Desenvolver pressupostos; Desenvolver a avaliação do risco; Determinar Medidas de Eficácia e de Performance; Determinar as Condições Decisivas; Determinar linhas de Operações.

São apontadas como uma oportunidade para aplicação de IA para facilitar os processos analíticos e desenvolvimento de estimativas até à elaboração do BAM.

Por outro lado, o desenvolvimento de CoA, quer da força opositora ou das nossas forças, com base em objetivos específicos que integrem todos os efeitos pretendidos no campo de batalha, e a realização do jogo da guerra para verificar e comparar modalidades de ação é também apontado como uma oportunidade para integrar seu processo IA (A. Lopes, *op. cit.)*. O objetivo da sua aplicação nesta situação é oferecer uma variedade de opções possíveis para que o decisor, enquanto humano, possa efetuar o processo de tomada de decisão (G. Vuocolo, *op. cit.*).

O fluxo de informação é também identificado como uma possível oportunidade para aplicação de IA agregando duas unidades de registo conforme Tabela 8:

Tabela 8 – Potencialidades para aplicação de IA relacionado com o fluxo de informação

Fluxo de informação	3.2.1 Redução de tempo
	3.2.2 Integração de diversas fontes

G. Vuocolo (*op. cit.*) aponta o emprego de IA com a digitalização da estrutura de C2 com vista a reduzir os tempos de reação oferecendo mais tempo para a avaliação da situação. No mesmo sentido, A. Pfaff (*op.cit.*), afirma que mesmo durante o decorrer das operações, o fluxo de informações que chega aos analistas pode ser de tal forma elevado que impossibilita a sua análise em tempo oportuno. Nesse sentido, a aplicação de IA para digerir todos estes novos dados, relacionando-os com vista à produção de informações válidas de forma célere, ou mesmo na deteção de padrões de conduta não percetíveis ao olho humano é vislumbrada como uma oportunidade para a sua aplicação.

Interligado com esta última, a possibilidade de integrar o fluxo de informação proveniente de diversas fontes ou sensores de forma organizada, configura-se uma mais valia e oportunidade (A. Pfaff, *op. cit.*).

Por conseguinte, as diversas potencialidades para a aplicação da IA são agrupadas por unidade de registo referentes a diversas técnicas de IA, conforme Tabela 9:

Tabela 9 – Potencialidades para aplicação por técnica de IA

Aplicação por técnica de IA	3.3.1 *Machine Learning*
	3.3.2 *Deep Learning*
	3.3.3 *Natural Language Processing*
	3.3.4 *Machine Vision*
	3.3.5 *Expert Systems*
	3.3.6 Outros

Em consequência das entrevistas realizadas verifica-se que ML, sendo a base para as restantes técnicas de IA, conforme referenciado na figura 3, pode ser empregue para classificação e sumarização de informações, elaboração de necessidades preditivas face a um determinado contexto, bem como, na previsão de alguns padrões e tendências com vista a desenvolver simulações. No que concerne ao DL, sendo esta uma técnica específica e mais aprofundada de ML, com capacidades muito mais amplas e eficazes no desenvolvimento de tarefas semelhantes no qual a grande diferença sustenta-se no número de parâmetros muito mais elevados que podem ser introduzidos (J. Carneiro, *op. cit.*).

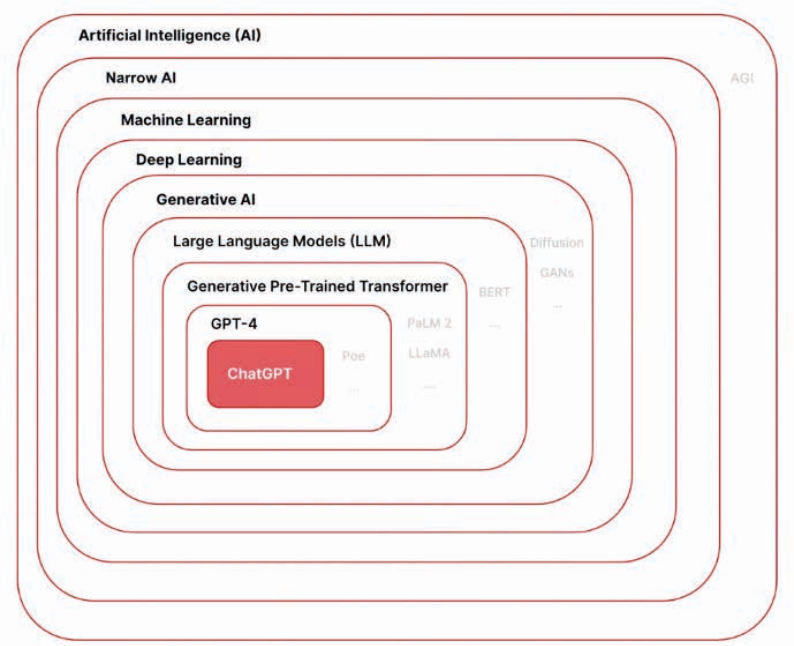

Figura 3 – Taxonomia da IA que relaciona
Fonte: Zwingmann (2023)

Por sua vez, o NLP, enquanto uma técnica específica do DL, foca-se na interação entre o operador humano e o próprio sistema de IA agilizando a comunicação entre ambos para dessa forma efetuar processamento de informações presentes em elevados volumes de dados, como por exemplo documentos ou áudios (J. Feijoo, *op. cit.*).

Corroborado por Konaev (2023, p. 13) o MV, enquanto outra técnica específica do DL, destaca-se pela sua capacidade de processar informação visual para detetar e identificar objetos ou pessoas, funcionando como olhos artificiais que capturam informação visual (R. Ribeiro, entrevista por videoconferência, 23 de fevereiro de 2024).

Por sua vez os ES "funcionam segundo um modelo procedimental, de acordo com um algoritmo fixado a priori e não reconfigurável (ao contrário da ML/DL), e como tal não dispõem da adaptabilidade destes últimos a situações em evolução rápida e caótica" (J. Feijoo, *op. cit.*). Não obstante, podem ser configurados e atualizados com novas regras e conhecimentos, semelhante à informação de um

especialista numa determinada área específica e serem empregues em contexto de simulações (J. Carneiro, *op. cit.*).

São ainda mencionadas outras técnicas de IA como os sistemas multiagentes com "capacidades de comunicarem entre si e com base nas informações que trocam entre si, podem tomar decisões. Ou seja, eles na realidade não são reativos, mas sim proativos" (J. Carneiro, *op. cit.*). Estes sistemas fornecem a capacidade de operar diversos meios interligados entre si, tal como o emprego de SANT em *swarm*[9] (Axe, 2023) ou captar a informação por determinados sensores que vão originar decisões em outros sistemas diferentes. Por norma este sistema encontra-se interligado a MV e NLP (J. Carneiro, *op. cit.*). A computação evolucionaria, por sua vez tem a capacidade de gerir e escalonar meios, sejam eles de transporte logísticos ou movimentos de forças de forma a otimizar rotas. (J. Carneiro, *op. cit.*). Por último, os modelos de IA generativa capaz de criar conteúdo como texto ou imagens, empregues na sumarização de documentos e extrair aspetos mais relevantes (J. Carneiro, *op. cit.*).

Em suma, alicerçado nos pontos fortes e potencialidades da IA elencados pelos entrevistados, demonstra-se o potencial transformador da IA no contexto militar, em particular na fase3 do SOCC-P2, onde precisão, eficiência e rapidez são fundamentais para o sucesso das operações. Assim, com as suas diversas técnicas e aplicações a IA apresenta ferramentas valiosas para enfrentar os desafios complexos do ambiente operacional moderno. Este desiderato sustenta-se como resposta à QD2: Quais as capacidades da IA com aplicação no SOCC-P2? E consequentemente é atingido o OE2.

4.4. Contributos para a otimização do SOCC-P2 através da Inteligência Artificial

Com as respostas às QD é possível relacionar eficazmente os dados recolhidos entre as dificuldades identificadas e possíveis soluções oferecidas com as potencialidades da IA, resolvendo desafios específicos e explorando o potencial de novas tecnologias.

As ferramentas da IA baseadas em ML e DL podem simplificar a utilização de ferramentas complexas, através da automação de tarefas complicadas e integração

[9] Baseia-se no comportamento coletivo de elementos em sistemas descentralizados e auto-organizados, ao seja, atuam em conjunto, tal como um enxame de abelhas através de IA (Russell, 2023).

de sistemas. Da mesma forma, podem ser elaborados interfaces com vista facilitar a interpretação e utilização de ferramentas mais complexas como por exemplo a identificação dos CoG, ou até como utilização da capacidade de simulação durante o jogo da guerra.

Por sua vez, a IA tem uma capacidade excecional de análise e sintetizar informações de diversas fontes, sejam elas em diversos formatos, com base em técnicas de ML, DL e NLP apoiando na integração de informação recolhida em diversas fontes. Que, por sua vez, pode apoiar na análise de elevados volumes de dados, reduzindo o tempo necessário para digerir elevadas quantidades de informação como por exemplo na análise do ambiente operacional através dos fatores: Político, Militar, Económico, Social, Informacional e Infraestruturas (PMESII) ou na análise de fatores, ou ainda para identificar padrões impossíveis de detetar manualmente em tempo útil, mostrando-se crucial para a compreensão do ambiente operacional.

Plataformas de IA, baseados em ES, podem ser empregues para apoiar no treino em tarefas específicas de planeamento com vista à rápida aquisição de competências. Por outro lado, pode ser amplamente empregue na parte da simulação como por exemplo em apoio no desenvolvimento de CoA e no jogo da guerra.

Noutra perspetiva, pode-se afirmar que a IA, através da automação de processos, apoio na análise de tarefas, assim como, na integração de várias plataformas vem de forma indireta apoiar na falta de recursos humanos.

Com vista a dar resposta à QC e cumprir o OG desta investigação que é propor contributos de como a IA pode otimizar o SOCC-P2, de seguida, apresentam-se de forma detalhada a aplicação das diversas técnicas de IA, conjugadas com as dificuldades na aplicação deste processo de planeamento conforme relatado pelos militares entrevistados, especificando como estas técnicas podem ser implementadas em cada etapa da fase 3 do SOCC-P2 detalhadas na figura 4, que pormenorizam o SOCC-P2 já ilustrado acima na Figura 2, presente no ponto 2.2.4.

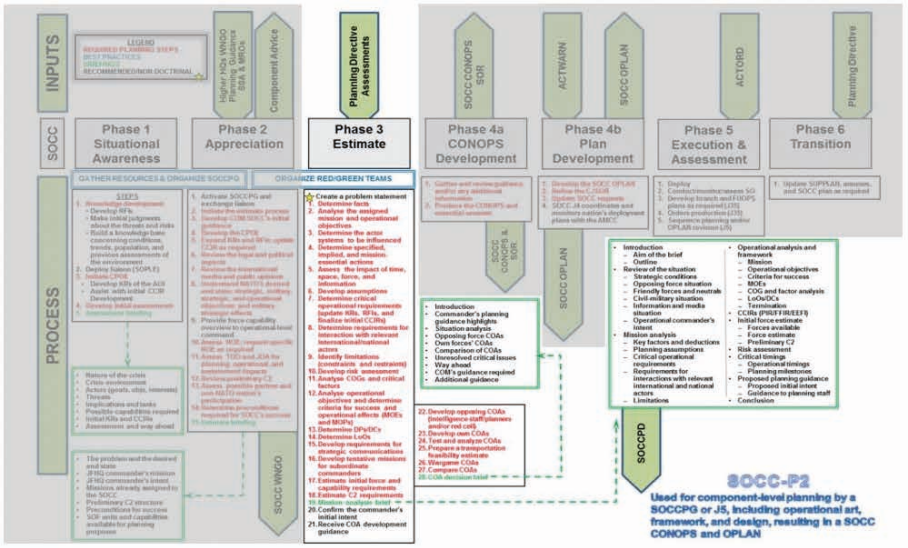

Figura 4 – Detalhe do SOCC-P2, com destaque para a fase 3
Fonte: NATO (2019, p. A-1).

Logo no início da fase 3, o NLP, ideal para processar grandes volumes de texto, pode ser empregue para processar e interpretar o *Operational Planning Guidance* e outras diretrizes, para extrair informações essenciais automaticamente apoiando os planeadores. *Comprehensive Understanding of the Operational Environment*[10] (CUOE) é uma tarefa que requere análise de uma vasta quantidade de informações dispersa em várias fontes, neste sentido a aplicação de ML e DL para analisar e relacionar informações identificando correlações complexas e padrões dificilmente percetíveis (*system of systems*), com vista a apoiar um entendimento mais célere abarcando uma maior quantidade de informação, facilitando a possível extração de objetivos, efeitos e ações a ser tidas em conta para o desenvolvimento do desenho de operações. Por sua vez, o MV pode ser aplicado para efetuar análise de dados geográficos e imagens satélites para compreender as condições ambientais e características do terreno.

[10] Adquisição e interpretação de conhecimento e compreensão do seu significado em relação a uma crise através do processo analítico coordenado para desenvolver um entendimento integrado das principais características do ambiente operacional, incluindo suas dimensões terrestres, aéreas/espaciais e marítimas, bem como os sistemas PMESII de adversários, amigos e atores neutros que possam influenciar operações conjuntas (NATO, 2019, p. F-6)

Da mesma forma, o ML pode apoiar na identificação e análise dos diversos atores e assim atribuir relações entre eles, apoiando na elaboração do diagrama de relações/influências entre atores. Subsequentemente, apoiar na identificação de mecanismos a alcançar para contribuir na resolução do problema materializado através do diagrama supracitado. Ainda, na análise dos fatores chave, tempo, espaço e força, o ML pode ser útil para apoiar na identificação de possíveis riscos ou limitações e através de IA generativa deduzir possíveis conclusões.

Relativamente ao desenvolvimento de pressupostos, verifica-se que a IA tem a capacidade de analisar informações incertas e preencher até lacunas de informação, nesse mesmo sentido a aplicação de IA generativa, pode apoiar na identificação de pressupostos.

Durante a análise do risco a aplicação de algoritmos de ML podem identificar padrões e indicadores de riscos, com base em dados históricos, e priorizá-los com base em dados estatísticos.

A determinação dos CoG, elencada como uma das dificuldades de análise, pode ser apoiada com algoritmos de ML e DL para determinar capacidades críticas, com base em dados históricos para identificar padrões de capacidade essenciais empregues e, desse ponto identificar possíveis requisitos e vulnerabilidades críticas.

Durante a elaboração do desenho de operações em que têm de ser estabelecidas as condições decisivas, diretamente relacionadas com efeitos e que, por sua vez, se encontram ligados a ações, os algoritmos de ML podem ser aplicados proporcionando uma base analítica de diferentes combinações, com base em históricos, a fim de otimizar este processo e prever a eficácia das condições decisivas. Por outro lado, os ES podem ser úteis para validar e fornecer recomendações baseadas em regras pré-estabelecidas e simular o desenho de operações para verificar a sequência e coerência das ações, efeitos e condições decisivas, com vista a atingir os objetivos estabelecidos. Consequentemente, estes mesmos algoritmos podem apoiar no desenvolvimento das CoA e mesmo efetuar o jogo da guerra com regras já predefinidas, com vista a identificar lacunas e otimizar as respetivas CoA das nossas forças.

Em síntese, a aplicação dos subcampos da IA nos passos específicos do SOCC-P2 acima referido possibilitam uma otimização deste PPO da NATO.

5. CONCLUSÕES

O impacto transformador das tecnologias de IA nas operações militares é inegável, com a IA a emergir como uma peça central na modernização das estratégias de defesa e segurança. O papel desempenhado da IA no conflito entre a Rússia e a Ucrânia é exemplo disso, quer na análise de grandes volumes de dados para gerar informações de elevado valor em tempo oportuno, contribuindo para a *Common Operational Picture,* quer na localização, deteção, identificação e reconhecimento de alvos através de imagens satélites e outros sensores contribuindo para o ciclo de *targeting*, ou ainda, na defesa contra ataques no ciberespaço e propaganda. Tais factos tornam urgente a necessidade de investir num sistema de C2 mais rápido e eficiente, capaz de gerir vastas quantidades de informações que possibilitem garantir uma vantagem estratégica e tomar as decisões em tempo oportuno.

De semelhante forma, o interesse por esta tecnologia despertou o interesse internacional levando a União Europeia e a NATO a desenvolver projetos no âmbito da defesa com aplicação de IA devido a sua evolução tecnológica e vantagem competitiva, para fazer face as ameaças modernas. No seguimento da linha de investigação identificada pela JSOU e em consonância das demais diretivas enquadrantes internacionais e internacionais, este trabalho focou-se na aplicação prática da IA no PPO da NATO, especificamente no contexto das OEsp, com o desiderato de otimizar o SOCC-P2.

A investigação adotou uma abordagem qualitativa, utilizando análise documental e entrevistas semiestruturadas como principais métodos de recolha de dados. A análise de conteúdo foi empregue para extrair significados dos dados recolhidos, orientados por um modelo analítico estruturado em torno dos OE estabelecidos e das QD.

Da análise efetuada é possível verificar que as principais dificuldades na aplicação do SOCC-P2, especificamente na fase 3, são a integração e análise do elevado volume de informações disponíveis e presentes em diversas fontes; a falta de pessoal especializado para conduzir o processo de planeamento; escassez de recursos humanos; e condicionamentos de tempo. Condicionando a qualidade e profundidade da análise da missão e elaboração das possíveis modalidades de ação durante a condução da fase 3 do processo de planeamento.

Por sua vez, a IA ostenta vantagens com a possibilidade de colmatar parte destes desafios mencionados, com particular interesse na capacidade de analisar e relacionar elevadas quantidades de dados e informações em tempo real, presentes

em diversas fontes, reduzindo o tempo e recursos humanos necessários no processamento dessa mesma informação.

Em paralelo, a IA presenteia ferramentas valiosas com potencial transformador no contexto militar, particularmente na fase 3 *Estimate* do SOCC-P2, das quais se salientam:

- NLP para o processamento de grandes volumes de texto com vista a analisar documentos recebidos pela cadeia de comando, como o *Operational Planning Guidance*.
- MV na análise de dados geográficos e imagens satélites para compreensão das condições ambientais e características do terreno.
- ML e DL para integrar analisar e relacionar informações presente em diversas fontes para apoiar o desenvolvimento do CUOE e consecutivamente do desenho de operações, assim como em apoio na determinação dos CoG.
- ML em apoio da identificação de atores e consecutivamente na elaboração do diagrama de relações e influências, bem como na análise dos fatores chave e ainda na identificação de limitações e priorização de possíveis riscos.
- IA generativa no apoio ao desenvolvimento de pressupostos e extração de conclusões das análises efetuadas.
- ES para simular o jogo da guerra a fim de validar e fornecer recomendações passíveis de introduzir no desenho de operações e refinar as CoA.

A integração destes algoritmos de IA nas tarefas apresentadas do SOCC-P2 otimiza a condução deste processo de planeamento pelas vantagens acima já apresentadas. Não obstante estes resultados, face à realidade das FFAA portuguesas, concretamente a CPOE, as integrações destes algoritmos teriam de ser numa versão *self contain,* com algoritmos mais simples e sem acesso a uma multiplicidade de fontes de recolha de informação. Dado que a utilização de uma *cloud* dedicada com a capacidade de interligar vários sensores e acesso às múltiplas fontes de informação ter um valor monetário demasiado elevado.

Como contributos para o conhecimento científico são identificados indicadores decorrentes da análise às entrevistas para futuras investigações concorrentes com este tema, sendo eles a dificuldade de análise, fator humano, recursos, vantagens, vulnerabilidades da IA, Processo de Planeamento, Fluxo de informação, Aplicação por técnica de IA.

Durante a fase exploratória e de análise foi possível confirmar o emprego de IA no conflito entre a Rússia e a Ucrânia de diversas formas, acima mencionadas, no entanto, face ao sigilo e confidencialidade do emprego desta nova tecnologia constituiu-se como uma limitação ao acesso da informação. No entanto a principal limitação deste estudo reside na rápida evolução tecnológica que pode alterar as premissas de algumas análises realizadas.

Com vista a dar continuidade a esta investigação, em futuros estudos sugere-se a análise focada na construção dos algoritmos identificados para concretizar a aplicação de IA na fase 3 do SOCC-P2.

Em paralelo às conclusões elencadas referentes à fase 3 do SOCC-P2, verifica-se que a IA tem ainda grande aplicação quer no ciclo de *targeting*, quer na fase 5 do processo de planeamento, conforme demonstrado na guerra Ucrânia. Nesse seguimento, face as potencialidades e vantagens da IA identificadas, em especial na capacidade de análise e relacionamento de elevadas quantidades de dados e informações em tempo real, através de diversos sensores interligados através de uma *cloud* dedicada recomenda-se como estudos futuros a integração de IA na fase 5 execução, do SOCC-P2 e consequentemente o emprego das mesmas em conflitos atuais enquanto estudo de caso, sendo exemplo disso o conflito de Israel.

REFERÊNCIAS BIBLIOGRÁFICAS

Axe, D. (2023, 28 de setembro). There Are So Many Explosives-Laden Drones Flying Over Southern Ukraine That They're Running Into Each Other [Página *online*]. Retirado de https://www.forbes.com/sites/davidaxe/2023/08/28/there-are-so-manyexplosives-laden-drones-flying-over-southern-ukraine-that-theyre-running-into-each-other/

Bauer, A. R. (2023). A new era of collective defence. *The Three Swords,* 39, 15. Retirado de https://www.jwc.nato.int/application/files/2616/9782/7206/issue_39 .pdf Bettencourt, R. (2022). Aplicação das tecnologias de inteligência artificial em operações militares (Trabalho de Investigação do Curso de promoção a Oficial General). Instituto Universitário Militar, Lisboa.

Branch, W. A. (2018). *Artificial Intelligence and Operational-Level Planning: An Emergent Convergence (Master's Thesis)*. School of Advanced Military Studies US Army Command and General Staff College, Fort Leavenworth, Kansas.

Breiner, J., & Ferran, M. (2024). *L-297 Loitering Munitions* (Munitions Safety Information Analysis Center). Germany: Munitions Safety Information Analysis Center

Comissão Europeia. (2020). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões*. (Estratégia da UE para a União da Segurança). Bruxelas: Autor. Ministério da Defesa Nacional. (2013). Conceito Estratégico de Defesa Nacional. Lisboa: Autor.

Dastin, J. (2023, 2 de fevereiro). Ukraine is using Palantir's software for «targeting» CEO says. [Online]. Retirado de https://www.reuters.com/technology/ukraine-is- using-palantirs-software-targeting-ceo-says-2023-02-02/

Estado-Maior General das Forças Armadas. (2022). *Diretiva Estratégica Setorial para as Operações Especiais nas Forças Armadas- 2022-2027*. Lisboa: Autor.

Estado-Maior General das Forças Armadas. (2023). Diretiva Estratégica do Estado-Maior- General das Forças Armadas 2023/2026. Lisboa: Autor.

European Defence Agency. (2021). Driven by global threats, shaped by civil high-tech, *European Defence Matters*, 22, 6. https://doi.org/10.2836/696496

Fontes, R., & Kamminga, J. (2023, 24 de março). *Ukraine A Living Lab for AI Warfare* [Online]. Retirado de https://www.nationaldefensemagazine.org/articles/2023/3/24/ukraine-a-living-lab-for-ai-warfare

Gillis, A. (2016). *What is Phishing? How Does it Work, Prevention, Examples*. *Security* [Online]. Retirado de https://www.techtarget.com/searchsecurity/definition/phishing

Gillis, A. (2023). *What is deep learning and how does it work? Definition from TechTarget*. *Enterprise AI* [Online]. Retirado de https://www.techtarget.com/search enterpriseai/definition/deep-learning-deep-neural-network

Giordano, P. (2023, 30 de outubro). Revolutionizing NATO Decision-Making. [Online]. Retirado de https://www.act.nato.int/article/revolutionizing-nato-decision- making/

Grady, A. C. (2023). Sharpening Our Competitive Edge. *Joint Force Quartely, 111*, 4th Quarter, 16-17.

Grzegorzewski, M. (2021). *Artificial Intelligence (AI) Factsheet*. Joint Special Operations University (JSOU) Quick Look. Retirado de https://jsou.libgiudes.com/jsoupublications

Hashemi-Pour, C. (2023). *What is Artificial General Intelligence? Definition from TechTarget. Enterprise AI* [Online]. Retirado de https://www.techtarget.com /searchenterpriseai/definition/artificialgeneralintelligence-AGI

International Business Machines Corporation (IBM). (2021). *What Is Machine Learning (ML)?* [Online]. Retirado de IBM. https://www.ibm.com/topics/ machine- learning

Kim, M. (2023). *The Convergence Algorithm – Leveraging Artificial Intelligence to Enable Multidomain Operations*. Military Review, 0026-4148, 6-9. Retirado de https://www.armyupress.army.mil/journals/military-review/online-exclu sive/ 2023- ole/the-convergence-algorithm/.pdf

Konaev, M. (2023). *Tomorrow's Technology in Today's War: The Use of AI and Autonomous Technologies in the War in Ukraine and Implications for Strategic Stability*. New York: Center for Naval Analyses

Laskowski, N. (2023). *What is Artificial Intelligence and How Does AI Work? Definition from TechTarget Enterprise AI* [Online]. Retirado de https://www. techtarget.com/searchenterpriseai/definition/AIArtificialIntelligence

Lutkevich, B. (2016). *What is Malware? Definition, Types, Prevention - TechTarget. Security* [Online]. Retirado de https://www.techtarget.com/searchsecurity/ definition/malware

Lutkevich, B. (2023a). *What Is an Expert System? Definition from TechTarget. Enterprise AI* [Online]. Retirado de https://www.techtarget.com/searchen terpriseai/def inition/expert-system

Lutkevich, B. (2023b). *What is Natural Language Processing? An Introduction to NLP. Enterprise AI* [Online]. Retirado de https://www.techtarget.com/search enterpriseai/definition/natural-language-processing-NLP

Milanovic, M. (2023). *Technology & Software Engineering – AI is not ChatGPT*. Retirado de https://www.linkedin.com/ posts/milanmilanovic_technologys oftwareengineeringchatgptactivity7089167368941137920p08s?utm_sour ce=share&utm_medium= member_desktop

North Atlantic Treaty Organization (NATO) (2022). *Strategic Concept*. NATO Summit. Madrid: Autor.

North Atlantic Treaty Organization (NATO) (2019). *Planning Handbook*. NATO Special Operations School. Mons, Belgium: NATO.

North Atlantic Treaty Organization (NATO) (2023). COPD V3.1 ACO *Comprehensive Operations Planning Directive*. Mons, Belgium: NATO.

North Atlantic Treaty Organization Special Operations Headquarters (NSHQ) (2014). *SOCC MANUAL,* Mons Belgium: NATO.

Pfaff, C. A., Lowrance, C. J., Washburn, B. M., & Carey, B. A. (2023). *Trusting AI: Integrating artificial intelligence into the Army's professional expert knowledge*. United States Army War College Press: Strategic Studies Institute.

Robinson, E., Egel, D., & Bailey, G. (2023). *Machine learning for operational decisionmaking in competition and conflict: A demonstration using the conflict in Eastern Ukraine* (Research Report) Santa Monica, California: Rand Corporation

Russell, S. (2023). AI weapons: Russia's war in Ukraine shows why the world must enact a ban. *Nature, 614*(7949), 620–623. https:/doi.org/10.1038/d41586-023-00511-5

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada Editora.

Simeral, S., Buckingham, M., Hughes, E., & Reisinger, R. (2022). Special Operations Research Topics 2023. JSOU *Press*, 27 Retirado de https://jsou.edu/Home/OpenFile?path=/Home/OpenFile?path=https://jsouapplicationstorage.blob.core.windows.net/press/437/JSOU_22_SORT23_final.pdf

Tucci, L. (2023). *What is Machine Learning and How Does It Work? In-Depth Guide – Enterprise AI* [Online]. Retirado de https://www.techtarget.com/searchenterpriseai/definition/machine-learning-ML

Watts, C. (2022, dezembro 3). Microsoft On the Issues – Preparing for a Russian cyber offensive against Ukraine this winter. Retirado de https://blogs.microsoft.com/on- the-issues/2022/12/03/preparing-russian-cyber-offensive-ukraine/

Yasar, K. (2023). What is Machine Vision? TechTarget – Enterprise AI [Online]. Retirado de https://www.techtarget.com/searchenterpriseai/definition/machine-vision-computer-vision

Yin, R. (2024) *Case Study Research. Design and Methods*. SAGE Publication, Inc. London. Zwingmann, T. (2023, 09 de junho). The Augmented Advantage – Demystifying AI: A Practical Guide to Key Terminology. Retirado de https://blog.tobiaszwingmann.com/p/demystifying-ai-practical-guide-key-terminology?ref=gptechblog.com

ESTUDO 4 – APLICAÇÃO DA INTELIGÊNCIA ARTIFICIAL AO SERVIÇO DA FUNÇÃO POLICIAL[1]

APPLYING ARTIFICIAL INTELLIGENCE TO THE POLICE

Pedro Manuel Sequeira Estrela Moleirinho
Coronel de Cavalaria da GNR

José Fontes
Docente na Academia Militar

RESUMO

A investigação tem como objeto de estudo a Inteligência Artificial aplicada aos Sistemas de Informação Geográfica na Guarda Nacional Republicana. A utilização das tecnologias de informação e comunicação tem vindo a promover uma alteração disruptiva na atuação policial, mormente na gestão e aplicação dos recursos no momento e local necessários. Assim, analisa-se o contributo da Inteligência Artificial na designada preditividade policial, fazendo uso dos Sistemas de Informação Geográfica para o desenho de um modelo concetual de cálculo do risco das diferentes tipologias criminais, pelo que este estudo apresenta interesse e utilidade para as Forças e Serviços de Segurança. Adotou-se uma abordagem multidisciplinar, aplicando-se o raciocínio indutivo, segundo uma estratégia de investigação qualitativa e como desenho de investigação o estudo de caso, realizando-se 20 entrevistas, sendo sete exploratórias e, as restantes, semiestruturadas de confirmação. Como principais contributos alcançados, salienta-se que o policiamento preditivo, utilizando a Inteligência Artificial, poderá *alavancar o produto operacional*. A Inteligência Artificial aplicada aos Sistemas de Informação Geográfica, em concreto aos Modelos de Risco do Terreno permitirá analisar o risco dos fenómenos criminais, capacitando uma melhor decisão e balanceamento proactivo de recursos da instituição para o seu combate.

Palavras-chave: Função Policial, Inteligência Artificial, Sistemas de Informação Geográfica

ABSTRACT

The investigation has as its object of study the Artificial Intelligence applied to the Geographic Information Systems in the Portuguese National Republican Guard. The use of information and

[1] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Promoção a Oficial General (CPOG 2020-2021). A versão integral encontra-se disponível nos Repositórios Científicos de Acesso Aberto de Portugal (https://www.rcaap.pt/).

communication technologies has made a disruptive change in police action, especially in the management and engagement of resources at the right time and place. Thus, the contribution of Artificial Intelligence to the so-called police predictiveness is analyzed, making use of Geographic Information Systems for the design of a conceptual model for risk calculation for different criminal typologies, so it is of institutional interest and usefulness for security forces and services. A multidisciplinary approach was adopted, applying inductive reasoning, according to a qualitative research strategy and the case study as a research design, with 20 interviews, seven of which were exploratory and, the rest, semi-structured for confirmation. As main contributions achieved, it is emphasized that predictive policing, using Artificial Intelligence, can leverage the operational product. The Artificial Intelligence applied to the Geographic Information Systems, in particularly to the Risk Terrain Models will permit the risk analysis of criminal phenomena, enabling a better decision and proactive balancing of institutional resources for its combat.

***Keywords**: Artificial Intelligence, Geographic Information Systems, Police Action*

1. INTRODUÇÃO

A temática das tecnologias de informação e comunicação (TIC) aplicada às várias realidades sociais e atividades humanas, é cada vez mais um interesse e imperativo de estudo transversal. Assume-se a dependência dos desenvolvimentos tecnológicos e pretende-se que estes alavanquem capacidades e competências, com eficiência e eficácia.

Também na atividade policial se procura *alavancar o produto operacional* com base neste "admirável mundo novo" (Huxley, 2013) das TIC, assumindo a Inteligência Artificial (IA) e a robotização um papel fulcral no desenvolvimento do policiamento preditivo (PP). A partir do ataque às Torres Gémeas, em Nova Iorque, em 2001, até ao ano de 2020: efetivamente, após estes fatídicos acontecimentos, a dimensão securitária do mundo sofreu alterações verdadeiramente marcantes. No campo da FP, considera-se verdadeiramente disruptiva a adoção de novas metodologias de atuação policial preditiva alicerçadas nas TIC, de que se destaca a IA. Relativamente ao limite do ano 2020, está-se ciente de que se encontra em fase de conceção a futura Estratégia da União Europeia (UE) para a IA, tendo sido, para já, propostas pelo Parlamento Europeu (PE) as diretrizes para a utilização civil e militar de IA, em 20 de janeiro de 2021 (PE, 2021). Posteriormente, em abril foi noticiado que a Comissão Europeia (CE) pretende regular a IA, sendo esta a primeira legislação

específica que visa atenuar os riscos tecnológicos e salvaguardar os valores dos direitos fundamentais da UE (Techaominuto, 2021).

Tem como objeto de estudo a IA aplicada aos Sistemas de Informação Geográfica (SIG) na Guarda Nacional Republicana (GNR). Assim, está-se perante a aplicação dos novos desenvolvimentos tecnológicos à Função Policial (FP)[2]. Analisa-se o contributo da IA na designada preditividade policial, fazendo uso dos SIG com o fito do desenho de um modelo concetual de cálculo do risco[3] para as diferentes tipologias criminais[4]. Considera-se a investigação alinhada com as opções estratégicas do Ministério da Administração Interna (MAI), bem como com as Linhas de Orientação Estratégicas da GNR, podendo contribuir para as opções de desenvolvimento das TIC nas Forças e Serviços de Segurança (FSS) dependentes do MAI, mais especificamente na GNR, crê-se apresentar utilidade ao nível doutrinário e também ao nível da sua aplicação.Relativamente à organização do estudo, além da presente introdução e das conclusões, no segundo capítulo apresentam-se as grandes áreas do conhecimento, que também se constituem como conceitos estruturantes: a FP, a IA e os SIG. Como anteriormente aflorado, aponta-se como centro de gravidade do estudo a FP, com escopo constitucional, mormente no que tange ao *direito à liberdade e à segurança*[5], como direito intrinsecamente ligado a esta função. Está, em aceso debate social, político e académico a aplicação das TIC a esta mesma atividade, na medida em que podem, precisamente, através da aplicação da IA, configurar-se como potencialmente lesiva dos mais elementares direitos fundamentais, com assinalável expressão no *direito à privacidade*[6].

---

[2] Cfr. al. e) do art.º 5. do Decreto-Lei n.º 249/2015, de 28 de outubro, que aprova a orgânica do ensino superior militar.

[3] Cfr. o conceito no Apêndice A.

[4] Cfr. o conceito no Apêndice A.

[5] Cfr. art.º 27.º da Constituição da República Portuguesa (CRP), aprovada pela Lei n.º 1/1976, de 10 de abril.

[6] Cfr. art.º 26.º outros direitos pessoais e art.º 35.º *direito da Informática*, da CRP.

Cruzam-se estas duas dimensões com a aplicação específica destas tecnologias e destas metodologias e técnicas preditivas de atuação policial aos SIG, com vista ao desenho de um modelo concetual de cálculo do risco para as diferentes tipologias criminais, a aplicar à GNR na sua área de atuação. Culmina-se este segundo capítulo com a exposição do modelo de análise.

No terceiro capítulo, explicam-se a metodologia e o método de investigação seguidos. No quarto capítulo, apresentam-se a análise dos dados e a discussão dos resultados, baseados nas entrevistas semiestruturadas de confirmação, contemplando as dimensões sociodemográficas política, estratégica, operacional e académica. Em resposta à questão derivada (QD) 1, abordam-se as áreas de aplicação da IA à atividade operacional das FSS, mormente da prevenção e da investigação criminais, explorando-se especificamente o modelo do PP. Como resposta à QD2, distinguem-se os limites legais, éticos e operacionais da aplicação da IA pelas FS em Portugal, tendo como pano de fundo os direitos fundamentais e os mecanismos de controlo e fiscalização internos e externos desta atividade. Após esta clarificação, analisa-se o papel dos SIG na construção de um mapa de risco da criminalidade, a partir do desenho de um modelo concetual de risco do terreno, respondendo-se à QD3. No final deste capítulo responde-se à QC.

2. ENQUADRAMENTO TEÓRICO E CONCETUAL

Atento o contexto do tema e a respetiva sinopse, irá explorar-se a componente operacional da FP das FSS, em particular da GNR, nas áreas da prevenção e da investigação criminais. Pretende-se uma abordagem à componente tecnológica em proveito desta mesma atividade, explorando-se as capacidades proporcionadas pela IA nas suas várias aplicações, especificamente o papel dos SIG para o desenho de um modelo concetual de cálculo do risco das diferentes tipologias criminais, na área de atuação da GNR.

Inicia-se com escopo nos fins do Estado de Direito democrático contemporâneo: a segurança, a justiça e o bem-estar (Sousa & Galvão, 2000, p. 25). No particular da segurança, Rodrigues e Santos afirmam que

> [no] atual modelo de Estado de direito democrático vigente no espaço europeu comunitário em que Portugal se insere, a segurança assume-se como um direito fundamental dos cidadãos, ganhando a dimensão de uma prestação essencial a que o Estado se encontra obrigado, num contexto que exige uma gestão estratégica cuidada,

> adaptada à realidade e dotada de instrumentos de apoio à decisão adequados. (2018, p. 83)

Para garantir globalmente estes fins, para além das outras atividades e instituições, o Estado Português garante a segurança na ordem interna, nos períodos de normalidade Constitucional, através das FSS, tal como previsto no art.º 272.º da CRP e no art.º 1.º da Lei de Segurança Interna (LSI), aprovada pela Lei n.º 53/2008, de 29 de agosto.

Esta garantia encontra prévia dignidade constitucional através do estabelecido no art.º 27.º *direito à liberdade e à segurança*. Este artigo é hodiernamente interpretado como um verdadeiro *direito garantia e também de contexto*. *Garantia* do cidadão poder exigir do Estado a sua proteção individual ou coletiva. Neste mesmo sentido Rosário (2013, p. 130) considera que é um "direito dos cidadãos a exigir dos poderes públicos a proteção dos seus direitos e existência de meios processuais adequados a tal"; de *contexto*, porque existem momentos em que o cidadão e a sociedade estão mais dispostos a abdicar do seu espaço de liberdade individual e coletiva, respetivamente, em detrimento da segurança e *vice-versa*.

Cumpre relevar que o *direito à liberdade e à segurança* ganhou esta dimensão humanista[7] ao ser contemplado na Declaração Universal dos Direitos Humanos e das Liberdades Fundamentais (DUDH) (Gouveia, 2014, p. 17)[8] e, mais tarde, na Convenção Europeia dos Direitos Humanos (CEDH)[9]. Desde aí, a sua aplicação tem experimentado diversas interpretações. Após os mediatizados ataques terroristas às Torres Gémeas, em Nova Iorque, tem-se verificado globalmente que os cidadãos têm estado mais disponíveis em abdicar do seu espaço de liberdade individual, em prol da segurança coletiva (Ratcliffe, 2016, pp. 41-44).

Esta garantia de segurança, promovida pelas instituições policiais no desenrolar da sua atividade diária — da secular vigilância da comunidade, tem vindo a aproveitar as capacidades proporcionadas pelas TIC, numa assumida alteração disruptiva das metodologias e técnicas de policiamento. Caetano (2008, p. 1166) afirmava, embora ao abrigo da Constituição de 1933, não perdendo,

---

[7] A *expressão direitos do homem foi substituída por direitos humanos*, cfr. o art.º 2.º da Lei n.º 45/2019, de 27 de junho. *Revisão global da linguagem utilizada nas convenções internacionais relevantes em matéria de direitos humanos*.

[8] Cfr. art.º 3.º *direito à vida, à liberdade e à segurança pessoal*. Aprovada pela Resolução n.º 217-A (III), de 10 de dezembro (1948).

[9] Cfr. art.º 5.º *direito à liberdade e à segurança*. Aprovada pela Resolução 2016/C 202/02, de 7 de junho.

contudo, atualidade, que o fito da vigilância "é a informação destinada a habilitar as autoridades de polícia a prevenir quaisquer possíveis perturbações e a adotar as necessárias providências para atalhá-las quando se produzam, ou para identificar os seus autores."

Estes modelos de policiamento mais preventivos têm vindo a utilizar as capacidades proporcionadas pelo acesso a grandes volumes de dados[10], o designado *big data*, e também da analítica fundamentada na IA. Ratcliffe (2016, p. 145) assume que a tecnologia facilitou: a análise de ADN; a análise das redes sociais e do tráfego telefónico; o movimento eletrónico de capitais; a videovigilância com reconhecimento facial; o movimento de pessoas em infraestruturas aeroportuárias e a leitura automática de matrículas.

Efetivamente, tem-se vindo a observar uma alteração disruptiva na atuação policial, nomeadamente na oportuna gestão e aplicação dos recursos, no local e no momento onde se tornem mais necessários.

Em contraponto, a aplicação destas mesmas tecnologias também tem vindo a ser questionada em diversos quadrantes — da dimensão política à dimensão jurídica, passando pela generalidade da sociedade. *Questiona-se o direito à privacidade ou da reserva da vida privada*, também este com dignidade constitucional, com previsão no art.º 26.º *outros direitos pessoais* e do art.º 35.º *direito da informática*, e igualmente contemplado na DUDH e na CEDH[11], nos artigos 12.º e 8.º, respetivamente. Como legislação *infra* constitucional, há ainda a destacar o art.º 80.º *direito à reserva sobre a intimidade da vida privada* do Código Civil, aprovado pelo Decreto-Lei n.º 47344/66, de 25 de novembro.

A recolha, o tratamento e a partilha dos dados pessoais no contexto da atividade policial, em geral, e da investigação criminal, em particular, tem vindo a ganhar aceso debate jurídico, operacional e social. No tocante ao direito fundamental da privacidade dos dados do cidadão, Hassemer (1995, p. 90) afirma que uma "política criminal que [...] disponha livremente da garantia da liberdade e da proteção dos direitos fundamentais com o propósito de ceder às exigências de um efectivo combate ao crime, coloca em jogo todas as tradições de Estado de direito." Em complemento, Monte (2013, p. 91) considera que "[a] modernidade, sobretudo com o advento do Estado de Direito formal, veio centrar o direito na

[10] Cfr. o conceito no Apêndice A.
[11] Cfr. art.º 8.º *direito ao respeito pela vida privada e familiar.*

proteção dos direitos individuais, corolário da enfatização do indivíduo e dos seus direitos pessoais."

Como enquadramento legislativo particular, cumpre apontar: a *Lei de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,* aprovada pela Lei n.º 58/2019, de 8 de agosto; e a *Lei de tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais,* aprovada pela Lei n.º 59/2019, de 8 de agosto.

Estes diplomas transpuseram para a ordem jurídica interna a Diretiva da UE 2016/680, de 27 de abril, *relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados,* abreviadamente designada por Regulamento Geral de Proteção de Dados (RGPD).

Sublinham-se os n.os 1 e 2 do art.º 23.º *tratamento de dados pessoais por entidades públicas para finalidades diferentes*, da Lei n.º 58/2019, de 8 de agosto, onde são taxativamente balizados o tratamento e a transmissão de dados pessoais por entidades públicas.

Também, tal como referido no n.º 1 do art.º 4.º *princípios gerais de proteção de dados,* da Lei n.º 59/2019, de 8 de agosto, "[o] tratamento de dados pessoais deve processar-se no estrito respeito pelos direitos, liberdades e garantias das pessoas singulares, em especial pelo direito à proteção dos dados pessoais."

É bem notório o elevado grau de exigência que se coloca às entidades públicas no tratamento dos dados pessoais, que, por maioria de razão, ganha alcance superior no desempenho das funções policiais.

Remetendo-se para os limites à atividade desenvolvida pelas FSS, em termos genéricos, esta atividade deve ser desempenhada tendo sempre presente o *princípio da proporcionalidade ou da proibição do excesso* (Canas, 2007, p. 449). Conscientes de que a atividade policial se desenvolve entre atos ampliativos e ablativos, este é um fino equilíbrio entre o prover segurança e o não ultrapassar esse mesmo fim – deve-se ter sempre presente o axioma da supremacia da lei.

Para além de se observarem os limites estabelecidos na lei penal, aprovado pelo Decreto-Lei n.º 48/95, de 15 de março e na LSI, também deve ser respeitado o *Código Deontológico do Serviço Policial*, aprovado pela Resolução do Conselho de Ministros (RCM) n.º 37/2002, de 7 de fevereiro.

Está também em causa a carga ética que a atividade policial deve encerrar. Mormente, as questões associadas à estigmatização, à discriminação e aos vieses,

bem como à falta de transparência (*black boxes*) relacionadas com a aplicação dos algoritmos[12] na FP. Maioritariamente destacam-se questões relacionadas com a raça e a etnia dos potenciais criminosos ou das eventuais vítimas (McDaniel & Pease, 2021, p. 10).

No caso particular da IA, considerando a *singularidade tecnológica*, em que "[...] a sucessão de inovações tecnológicas cada vez mais rápidas conduzirá a uma alteração tão profunda e tão rápida da sociedade, que se torna impossível prever o [...] nosso futuro para além de um dado instante no tempo [...]" (Oliveira, 2018), teme-se a entrada numa nova dimensão de *algoritmocracia* (J. Magalhães, entrevista por *Zoom*, 1 de março de 2021).

Magrani (2018, p. 178) também considera que na conceção algorítmica se deve pensar segundo os princípios da privacidade, da segurança e da ética. Complementarmente, Fontes (2015, p. 42) afirma que "[o] Estado, os seus órgãos e agentes sabem que é nas situações de maior fragilidade e dependência que a superioridade ética assume particular relevância."

Para assegurar esse mesmo cumprimento, existe um conjunto de mecanismos de controlo e fiscalização internos e externos da atividade policial. No caso da GNR, internamente, para além da restante hierarquia, os mesmos são tutelados pela Inspeção da Guarda (IG) e pela Direção de Justiça e Disciplina. Externamente, todas as FSS dependentes do MAI têm como mecanismos a Inspeção Geral da Administração Interna (IGAI) e, em paridade, os Tribunais, não se podendo descurar também o escrutínio da opinião pública e da comunicação social.

Como grandes áreas de intervenção da exigente atividade diária das FSS, assinalam-se: "informações; prevenção; manutenção ou reposição da situação de legalidade e segurança e investigação criminal" (Silva, 2010, p.15).

No particular da GNR, conforme estabelecido na *Estratégia da Guarda – Uma Estratégia Centrada nas Pessoas,* as respetivas áreas de intervenção são "a policial, a de segurança e ordem pública, a de fiscalização da circulação rodoviária e a de investigação criminal e contraordenacional" (GNR, 2020, p. 27).

Novamente com enfoque na aplicação das tecnologias à FP, Brynjolfsson e McAfee (2020, p. 36) afirmam que "a [IA], em especial a aprendizagem computacional, é a maior tecnologia de âmbito geral da nossa era." Em termos históricos, esta tecnologia foi pela primeira vez referenciada por John McCarthy, em 1955. Desde aí

[12] Cfr. o conceito no Apêndice A.

foi evoluindo progressivamente, tornando-se verdadeiramente galopante a partir de 2016, com o desenvolvimento e aperfeiçoamento da aprendizagem de máquina (AM)[13], baseada em redes neuronais (Brynjolfsson & McAfee, 2020, pp. 21-22).

As suas aplicações têm sido transversais a todas as áreas do conhecimento, começando também a ganhar sustentação em diversas aplicações ao dispor das FSS.

Raaijmakers (2019, p. 74) apresenta como aplicações de IA de utilização mais comum pelas FSS: identificação de perfis de suspeitos; controlo de tráfego; análise de movimentos bancários na *dark web*; deteção de pornografia infantil e deteção de padrões anormais na vigilância de espaços públicos.

Genericamente, pretende-se que estas novas capacidades preditivas *alavanquem* a atividade operacional, permitindo, em paridade, uma melhor capacidade de comando e controlo (C2) e de decisão, na alocação e balanceamento de recursos. O PP assenta as suas metodologias na análise e na avaliação do risco. Para tal, o volume, a qualidade dos dados e das informações são importantes para potenciar a capacidade tecnológica e analítica deste modelo de atuação policial. Assim, o PP faz uso de modelos computacionais, com base na criminalidade ocorrida e nos dados do contexto ambiental, para aferir a probabilidade das ocorrências criminais futuras.

Tal como estabelecido por Perry et al., (2013, p. xiv) e reproduzido na Figura 1, o processo de gestão do policiamento orientado pela predição é um ciclo de quatro etapas: as duas primeiras são a recolha e a análise da fusão de dados relativos a crimes, a incidentes e a infratores, para que se possam formular as predições; a terceira consiste em realizar operações policiais que tenham impacto no crime previsto; na quarta, as intervenções levam à redução e irradicação da criminalidade.

[13] Tradução do Autor de "*machine learning*". Cfr. o conceito no Apêndice A.

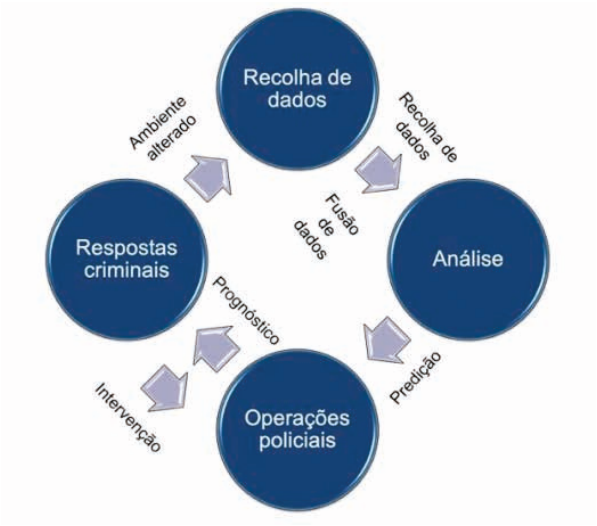

Figura 1 – Policiamento orientado pela predição
Fonte: Adaptado a partir de Perry et al. (2013, p. 128).

Existem quatro categorias de métodos de PP: métodos de predição do crime; métodos de predição dos criminosos; métodos de predição do *profiling* dos criminosos e métodos de predição das vítimas de crime. Ribeiro (2018, p. 89) alerta que "[a] previsão não é apenas acerca do onde e quando, necessita também da explicação (porquê) para se determinar o que fazer para contrariar a atividade [...]".

Considerando a atual variedade de sensores, tipologias e quantidade de dados — que Campbell (2018, p. 2) alegoricamente refere como *tsunami tecnológico* —, aliados à sua qualidade e capacidade analíticas, vão permitir incrementar a capacidade preditiva das FSS. Na última década, com o desenvolvimento da IA, destacando-se, como salientado, a AM, será preciso aferir a legitimidade da sua cabal adoção pelas FSS.

Cabral et al. (2018, pp. 232-233) apresentam como exemplos de modelos de boa gestão utilizando estas tecnologias pelas FSS: a definição das áreas e dos percursos de patrulhamento; o estudo das diferentes estratégias de policiamento e os horários e configuração das patrulhas.

Em contraponto, num estudo científico de avaliação do PP relativamente à redução da criminalidade, realizado por Ratcliffe et al. (2020, p. 23), na cidade de Filadélfia, no qual foi utilizado um *software* de AM, é afirmado que o PP pode melhorar a precisão da atuação policial, mas estes mecanismos analíticos de prevenção devem ser transparentes e democráticos.

Também Fernandes (2020, p. 34), apesar de identificar vantagens na aplicação do PP, considera que poderá ser difícil avaliar a sua eficácia relativamente à "quantificação do impacto direto das medidas implementadas na diminuição do crime". Porque é "árdua a tarefa de determinar se a diminuição do crime ocorreu devido às medidas implementadas ou se existem outros fatores a contribuir para [essa] diminuição [...]."

No seguimento, os critérios de boa gestão consubstanciam-se em alocar os recursos policiais aos locais onde exista uma maior probabilidade do crime vir a ocorrer. Esta probabilidade baseia-se numa análise e avaliação do risco[14], considerando as variáveis espaço, tempo e oportunidade, conforme ilustrado na Figura 2:

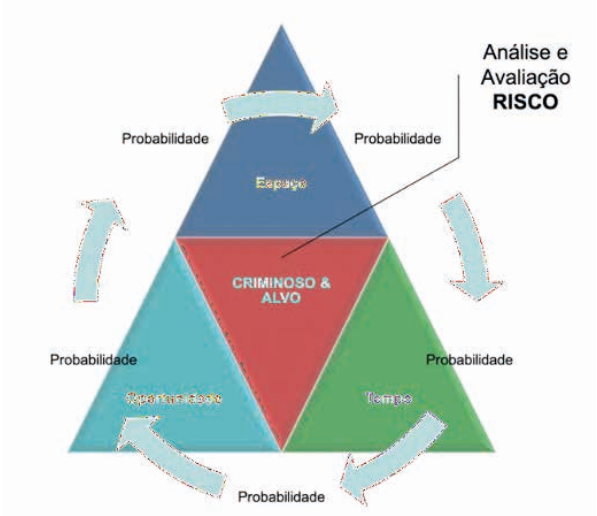

Figura 2 – Triângulo do crime
Fonte: Adaptado a partir de João et al., (2013, p. 139).

[14] Cfr. o conceito no Apêndice A.

Como afirmam João, Lobo e Bação (2013, p. 139), "o conhecimento exacto onde os crimes são praticados pode contribuir para um plano mais eficaz de prevenção."

Uma das formas das FSS potenciarem a sua capacidade preditiva e que tem experimentado assinalável progressão, reside no crime *mapping* através da utilização dos SIG com vista a melhor analisarem e avaliarem os respetivos riscos.

Os SIG iniciaram o seu percurso histórico em 1829, em França, por Adriano Balbi e Andre-Michel Guerry, relacionando o crime com os níveis de escolaridade da população (Weisburd et al., 2009, p. 3).

A partir de 1960, a elaboração manual dos mapas deu lugar à utilização dos computadores, ainda que com as limitações inerentes às respetivas capacidades da época (Harries, 1999, p.91). Wilson e Filbert (2017, p. 373) assumem que a terminologia *mapeamento do crime*, pode ser demasiado simplista por apenas ser associada a uma mera visualização dos dados criminais num SIG. Mas o termo também contempla os aspetos técnicos de estatística, os princípios geográficos e as teorias criminológicas. Para estes Autores, o *mapeamento do crime* conjuga duas dimensões: a técnica, que combina as metodologias de mapeamento e análise espacial de dados; e a teórica, que resulta da análise conjugada da geografia, da sociologia e da criminologia.

Assim, as causas *situacionais do crime,* ligadas ao histórico social do criminoso, têm mais sucesso na redução da criminalidade a curto prazo porque a relação causa-efeito é mais direta (McDaniel & Pease, 2021, p. 11).

Complementarmente, para Caplan (2014, p. 10) a *influência ambiental* refere-se à forma como as caraterísticas de determinado local afetam outros locais circundantes. Existem evidências de que alguns eventos criminais cometidos em determinada área geográfica estão relacionados com um número reduzido de criminosos reincidentes e um número circunscrito de vítimas recorrentes (McDaniel & Pease, 2021, p. 12).

Na análise tática, o *mapeamento do crime* pode ser empregue para identificar padrões de proximidade de criminalidade, nomeadamente contra o património e o roubo (Santos, 2016, p. 161). Para Ribeiro (2018, p. 87), adicionalmente estas ferramentas têm um papel preponderante na tomada de decisão, pois permitem o cruzamento dos dados e a projeção georreferenciada de eventos futuros.

Como afiançam Neto et al. (2018, p. 305), a mais-valia dos SIG reside na capacidade de integrar a tecnologia de apoio à decisão espacial nas decisões

críticas. Porém, alertam que "[as] fontes de dados necessárias, que por vezes são provenientes de diferentes sistemas e operadas por diferentes agentes, tornam a tarefa do SIG num desafio." Pretende-se que os SIG sejam plataformas de apoio à decisão apelativas e intuitivas, apresentando-se sob a forma de *dashboards*. Estes possibilitam "a monitorização, visualização e análise da informação crítica no suporte à decisão, de uma forma simples e objetiva, permitindo a revelação de relações que seria difícil identificar analisando cada dimensão individualmente" (Neto et al., 2018, p. 311).

As FSS que utilizam estas plataformas conseguem analisar os dados estatísticos para precisar a localização dos crimes e dos acidentes rodoviários e as respetivas flutuações estatísticas, possibilitando alocar recursos ao seu combate futuro (Neto et al., 2018, p. 305). Apresenta-se na Figura 3 o processo autoexplicativo de *mapeamento do crime* pelos SIG:

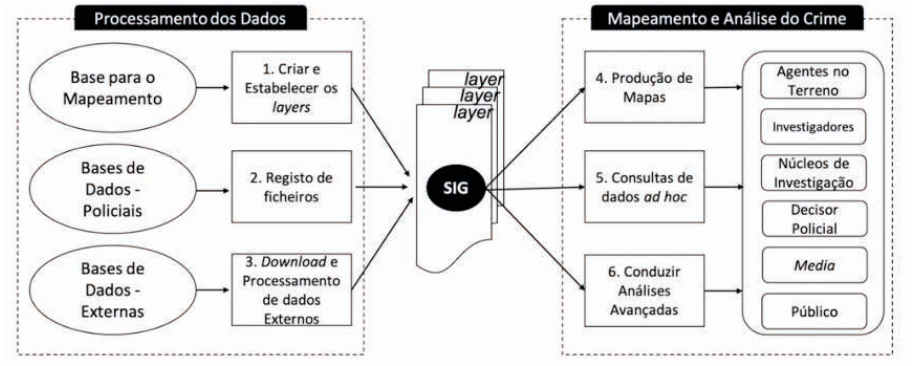

Figura 3 – Processo de *mapeamento do crime* pelos SIG
Fonte: Adaptado por Gonçalves (2020, p. 21) de *International Association of Crime Analysts* (2012).

Atualmente, assiste-se a uma nova dimensão de aplicação dos SIG. Passou-se da mera marcação de pontos no mapa, que apenas graficavam eventos passados, para a construção de Modelos de Risco do Terreno (MRT)[15] com capacidade de prospetiva e predição de novos eventos criminais. Assim, o MRT é uma técnica do PP que permite antecipar eventos criminais, balanceando-se com oportunidade os recursos segundo os critérios de boa gestão (Piza, Caplan, & Kennedy, 2011, pp. 339-340).

[15] Tradução do Autor de "Risk Terrain Modelling (RTM)".

Concetualmente, os MRT são uma metodologia de avaliação do risco, através da sobreposição de diferentes camadas que representam a influência espacial de determinadas caraterísticas de uma região, sendo estas apresentadas através de um SIG. Estes mapas identificam os riscos de determinada região e modelam a forma de relacionamento espacial para simularem configurações de eventos criminais futuros (Caplan, 2014, p. 10).

Os MRT assentam o seu desenvolvimento em três pilares: o risco, o terreno e a modelação (Caplan & Kennedy, 2011, p. 68).

Anyinam (2015, p. 26) afirma que os MRT têm como resultado mapas geoespaciais de *hot spots* de probabilidade de ocorrências criminais, num determinado espaço temporal. Estes mapas, para além de identificarem os *hot spots*, também permitem saber o que é que pode ser feito para mitigar o risco (Caplan, 2014, p. 12).

Em suma, estes mapas analisam os locais que contribuem para a concentração da criminalidade, identificando as janelas de oportunidade para o seu cometimento futuro.

Cumpre salientar que na sua construção apenas dever ser contemplada uma única tipologia criminal, pois estas têm caraterísticas e fatores de risco e ambientais próprios (Vilhena, 2019, p. 23). Neste mesmo sentido, Fernandes (2020, p. 34) relata que "[as] previsões relativas ao risco criminal são, em regra, apresentadas por tipo de crime (por exemplo, furto de viaturas, roubo na via pública ou furto do interior de residências)."

Johnson (2017, p. 108, p. 199) acrescenta que o *mapeamento do crime* e a análise espacial se têm vindo a tornar ferramentas preponderantes para os analistas criminais e para os académicos. Assim, permite-se assumir os SIG como uma relevante ferramenta de apoio à decisão no tocante à segurança, de uma forma geral, e à prevenção e investigação criminal, em particular (Ferreira & Martins, 2011, p. 615). Os SIG capacitam as FSS para o estabelecimento de relações entre as ocorrências criminais e as restantes variáveis, apurando padrões e definindo áreas prioritárias de intervenção.

Associando a IA aos SIG, salienta-se que esta combinação possibilitará uma superior capacidade analítica de grandes volumes de dados e um refinamento exponencial da predição. Contudo, cumpre notar que a IA pode ser uma componente importante do PP e, particularmente, na atual conceção dos SIG, mas ambos são conceitos distintos (McDaniel & Pease, 2021, p. 2).

Relativamente à plataforma de georreferenciação da GNR, o Sistema Integrado de Informações Operacionais de Polícia — Georreferenciação (SIIOP-G), Alexandre (2014, p. 34) refere que o "sistema é decisivo para simular cenários de ocorrências, avaliar os impactos das intervenções, efectuar mapas das ocorrências, produzir mapas de risco 'pontos negros' (real, potencial e resultante da percepção de risco pelos habitantes)." Considera também que o SIG é fundamental para o sistema de apoio à decisão da GNR (Alexandre, 2014, p. 37).

Apresenta-se na Figura 4 o Processo autoexplicativo de *mapeamento do crime* realizado na GNR.

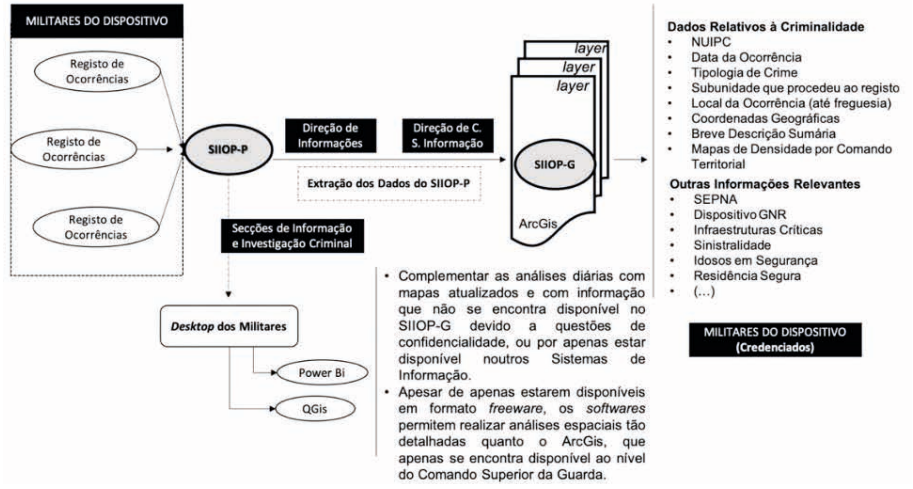

Figura 4 – Processo de *mapeamento do crime* realizado na GNR
Fonte: Gonçalves (2020, p. XXVIII).

Temos presente que a versão 4.0 do SIIOP-G, prevista para 2025, pretende apresentar contributos para a implementação do policiamento orientado pelas informações, para o *geoprofiling*, para o mapeamento criminal e para a análise preditiva. (J. Nunes, entrevista por *email*, 07 de novembro de 2020).

2.1.2. Conceitos estruturantes

Seguidamente, apesar de já terem sido aludidos, adota-se e fixa-se um quadro de referência de conceitos estruturantes e auxiliares[16]:

[16] Para cada um dos conceitos estruturantes: FP, IA e SIG, são associados os respetivos conceitos auxiliares que se encontram plasmados no Apêndice A.

2.1.2.1. Função Policial

O conceito de Polícia encontra dignidade constitucional no art.º 272.º. Ainda assim, Canas afirma que

> [o] artigo 272.º, n.º 1, é ambíguo. A noção de polícia que incorpora não é clara: trata-se de polícia em sentido material ou funcional (atividade ou função de polícia, praticada pela Administração), ou de polícia(s) em sentido orgânico (os vários órgãos e serviços da Administração que desempenham dominantemente funções materiais de polícia). (2007, p. 454)

Nesse mesmo sentido, Raposo refere que

> [não] é fácil definir a polícia enquanto atividade. Poder-se-á, no entanto, partir da ideia de que a polícia em sentido material que consiste no modo atuação administrativa destinada a prevenir os perigos que ameaçam determinados bens jurídicos. Na economia do artigo 272.º n.º 1, da Constituição, a legalidade democrática, a Segurança Interna [SI] e os direitos dos cidadãos.

(...) A atividade policial incide sobre os comportamentos humanos suscetíveis de afetar interesses gerais. (2013, p.283)

Como complementa Valente,

> [a] essência legitimadora e limitadora da atividade de polícia é de natureza constitucional com a consagração de um duplo dever ser — defender e garantir (que implica respeitar) — e de uma tríplice dinâmica material — legalidade democrática, [SI] e direitos de todos os cidadãos (vítima, indiciado, cidadão em geral). (2014, pp. 44-45)

Ainda assim, como função ou atividade desenvolvida pela polícia, assume-se a definição apresentada por Caetano (2008, p. 1150), aí identificava-se que "as leis procuram evitar e prevenir os danos sociais", sendo o "modo de actuar da autoridade administrativa que consiste em intervir no exercício das actividades individuais susceptíveis de fazer perigar interesses gerais, tendo por objectivo evitar que se produzam, ampliem ou generalizem os danos sociais que as leis procuram prevenir".

Numa concetualização mais atual, Castro estabelece que na doutrina nacional o conceito de polícia, pode ser analisado em várias perspetivas:

> na perspectiva da atividade material de polícia, que pressupõe uma finalidade própria, distinta das demais formas de atividade

> administrativa que concorrem para a satisfação do interesse público, e num sentido orgânico ou institucional, enquanto conjunto de órgãos e agentes pertencentes a serviços administrativos cuja função essencial consiste no desempenho de tarefas materiais de polícia. (2003, p. 30)

Em resumo, a Polícia é, em simultâneo, uma atividade e um órgão administrativo, que deve ter sempre presente uma observação rigorosa do *princípio da proporcionalidade* ou da *proibição do excesso*, tal como decorre do art.º 272.º, n.º 2, da CRP, "[as] medidas de polícia são as previstas na lei, não devendo ser utilizadas para além do estritamente necessário."

2.1.2.2. Inteligência Artificial

Conforme preconizado pela UE (CE, 2020, p. 2) no *Livro Branco sobre a inteligência artificial:* "a IA é um conjunto de tecnologias que combinam dados, algoritmos e capacidade computacional. Os progressos em computação e a cada vez maior disponibilidade de dados são, por conseguinte, os principais motores do atual impulso da IA."

Em complemento, "[o] conceito de [IA] aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas – com um determinado nível de autonomia – para atingir objetivos específicos" (CE, 2018).

Já o PE (2020) advoga que "[a] IA é a capacidade de uma máquina para reproduzir competências semelhantes às humanas como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade."

Atento às capacidades dos seus algoritmos, a IA pode ser classificada em *limitada, geral* e *super*. Em termos de aplicação à FP, assume-se que esta se encontra no primeiro patamar, *i. e.*, limitada, pelo que devemos ter alguma contenção quanto à utilização generalizada do termo IA neste contexto (McDaniel & Pease, 2021, pp. 18 e 19).

Segundo um estudo do Eurobarómetro realizado nos, então, 28 Estados da UE, em 2017, "61% dos europeus têm uma opinião positiva sobre a inteligência artificial, mas 88% consideram que estas tecnologias exigem uma gestão com cautela" (PE, 2020).

No seguimento da cautela, para além dos limites legais da utilização da IA, em paridade, também devem ser considerados os limites éticos. Relativamente aos

limites legais, Magrani (2019, p. 27) considera que a tecnologia está a desenvolver-se com mais rapidez do que a nossa capacidade para assegurar a tutela dos direitos individuais e coletivos.

Floridi e Cowls (2019, p. 2) afirmam que existem organizações que tiveram múltiplas iniciativas para estabelecer princípios éticos na utilização da IA, mas o seu volume pode tornar-se excessivo e criar dificuldades na sua aplicação.

Resultante da análise comparativa de 47 princípios relacionados com a bioética, aqueles Autores sintetizaram-nos em cinco: a beneficência, a prevenção de danos, a autonomia, a justiça e a explicabilidade.

Tal como refere Fernandes (2021, p. 58), o *enquadramento unificado dos cinco princípios para a IA na sociedade,* resultante da investigação daqueles autores "pode servir como enquadramento para o processo de definição de melhores práticas, padrões técnicos, regulamentos ou legislação relativa ao recurso à IA nos diversos setores públicos."

Ainda no tocante às questões éticas, cumpre relevar que foi criado pela CE (2021) um grupo de especialistas de alto nível sobre IA, constituído por representantes da academia, da sociedade civil e da indústria. Este grupo teve um trabalho central para o desenvolvimento de algumas das iniciativas políticas europeias sobre o tema, nomeadamente: *Building Trust in Human Centric Artificial Intelligence; White paper on Artificial Intelligence: a European approach to excellence and trust e Coordinated plan on AI*.

2.1.2.3. Sistema de Informação Geográfica

Conforme Santos (2013, p. 5), um SIG é um conjunto de aplicações informáticas que permitem modificar, visualizar, consultar e analisar dados geográficos. Estas ferramentas conseguem mapear o crime de diversas formas, do mais simples mapa de pontos, até às representações tridimensionais de dados espaciais ou temporais.

Estas poderosas ferramentas de mapeamento digital do crime servem para identificar *hot spots* e *hot people* de criminalidade em tempo real, através de algoritmos de identificação de padrões em grandes bases de dados policiais (McDaniel & Pease, 2021, p. i).

Em resumo, sistematiza-se ora o relacionamento entre as diversas áreas de conhecimento e dos respetivos conceitos estruturantes e auxiliares *supra* identificados.

Assim, assume-se como centro de gravidade a FP, com as suas diversas declinações: a SI[17], as FSS e, por fim, o enfoque na GNR. Esta função num Estado de direito democrático moderno, em cumprimento dos seus fins[18], alicerçada no *princípio da separação de poderes*[19] e no *império da lei*, está intimamente exposta a um *sistema de freios e contrapesos*: legais, éticos e operacionais.

Sob este escopo, a FP experimenta hoje capacidades técnicas de atuação proporcionadas pelas TIC, com especial destaque para a IA aplicada aos SIG, que lhe permite refinar com superior eficiência a análise e avaliação do risco nas áreas da prevenção e da investigação criminais, com expressão no designado PP.

Apresenta-se graficamente o contexto do estudo na Figura 5.

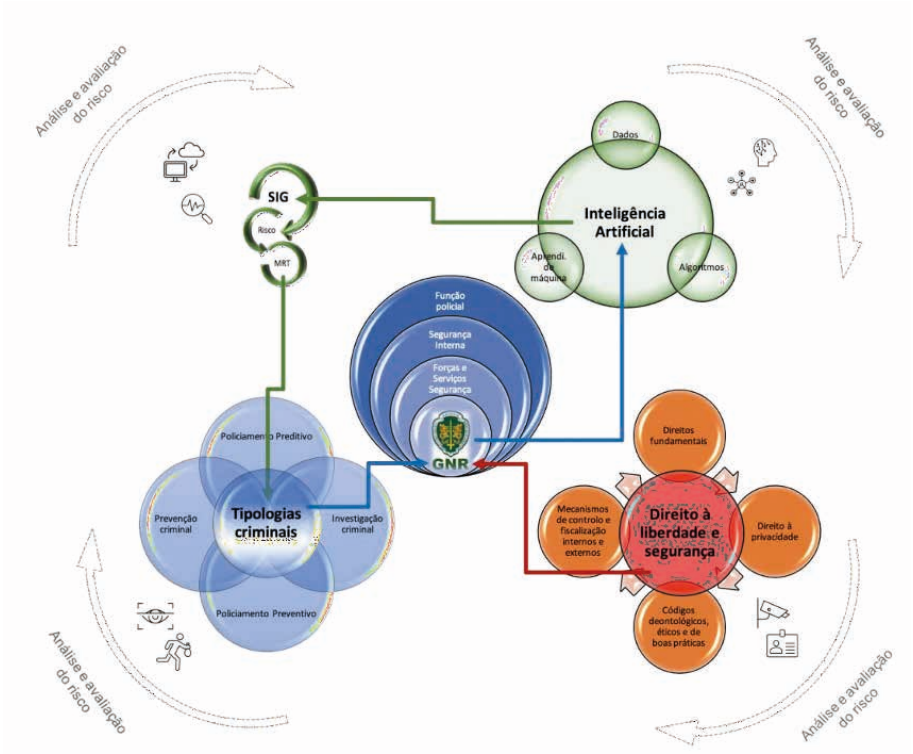

Figura 4 – Processo de *mapeamento do crime* realizado na GNR
Fonte: Gonçalves (2020, p. XXVIII).

[17] Cfr. o conceito no Apêndice A.
[18] De segurança, justiça e bem-estar.
[19] Legislativo, executivo e judicial.

2.2. Modelo de análise

Após o levantamento do estado da arte e o enquadramento teórico, com referência aos conceitos adotados, apresenta-se o modelo de análise.

Quadro 1 – Modelo de análise

Tema	Aplicação da IA ao serviço da FP.					
OG	Analisar o modelo de integração da IA aplicada aos SIG na GNR.					
OE	QC	Como potenciar a IA aplicada aos SIG na área de atuação da GNR?			Recolha de dados	
	QD	Conceitos[29]	Dimensões	Indicadores	Inst. recolha	Técn. análise
OE1 Analisar as áreas de aplicação da IA à atividade operacional das FSS.	**QD1** Quais as áreas de aplicação da IA à atividade operacional das FSS?	- IA - Dados - Algoritmos - AM - Aprendizagem profunda - FP - Atividade operacional	- Prevenção criminal - Investigação criminal	- Policiamento preventivo - PP - Análise e avaliação do risco	- Análise documental - Entrevistas exploratórias - Entrevistas semiestruturadas - *Elite Interviewing*	- Qualitativa
OE2 Distinguir os limites legais, éticos e operacionais da aplicação da IA pelas FS em Portugal.	**QD2** Quais os limites legais, éticos e operacionais da aplicação da IA pelas FS em Portugal?	- Lei - Ética - SI - Polícia - FS	- SI - Atividade operacional	- Direitos fundamentais - Direito à privacidade - Códigos deontológicos, éticos e de boas práticas - Mecanismos de controlo e fiscalização internos e externos		
OE3 Analisar o papel dos SIG para a construção de um mapa de risco da criminalidade na área de atuação da GNR.	**QD3** Qual o papel dos SIG na construção de um mapa de risco da criminalidade na área de atuação da GNR?	- SIG - Risco - Criminalidade - Investigação criminal	- Prevenção criminal - Investigação criminal	- Sistemas de apoio à decisão - Análise de informação criminal		

3. METODOLOGIA E MÉTODO

No tocante à posição filosófica, assumiu-se a ontológica construtivista, uma vez que a aplicação da IA na GNR, considerando o estudo de caso de um modelo concetual de cálculo do risco das diferentes tipologias criminais, resulta da interação de diversos atores sociais num contexto em constante mutação (Bryman, 2012, pp. 33-35).

Em paridade, assumiu-se uma posição epistemológica interpretativista, na medida em que, para além de se aferirem os fenómenos sociais ligados à factualidade criminal, também se compreendeu e interpretou a sua subjetividade relativa (Santos & Lima, 2019, p. 18).

Aplicou-se o raciocínio indutivo, partindo-se da observação de factos particulares para posteriormente se estabelecerem generalizações (Santos & Lima, 2019, p. 18).

Logo, observaram-se os atuais desenvolvimentos da IA aplicada aos SIG nas FSS, mormente o seu particular contributo no desenho de um modelo concetual de cálculo de risco das diferentes tipologias criminais. E, finalmente, estabeleceu-

se, por associação, a sua aplicação generalizada à atividade de prevenção e investigação criminais na GNR.

Apesar de se assumir este raciocínio indutivo, acompanha-se Freixo (2009, p. 99) quando afirma, relativamente aos métodos dedutivo e indutivo, que estes não se opõem entre si e que até se podem complementar.

Na senda, adotou-se uma estratégia de investigação qualitativa, porque, considerando a natureza do objeto e os objetivos do estudo, não é possível traduzir em números as relações entre o contexto real e os elementos subjetivos do sujeito (Santos & Lima, 2019, pp. 27-29). Após a definição da estratégia de investigação, assumiu-se como correspondente desenho de investigação o estudo de caso para se proceder à recolha e análise de dados (Santos & Lima, 2019, pp. 61-63).

No caso vertente, abordou-se especificamente o estudo de caso do desenho de um modelo concetual de cálculo de risco das diferentes tipologias criminais, através da aplicação da IA aos SIG pela GNR na sua área de atuação.

No tocante à análise e à apresentação dos dados e à avaliação e à discussão dos resultados, além do já aduzido, cumpriu-se o estabelecido por Santos e Lima (2019, pp. 91-142).

Seguidamente caraterizam-se os participantes, o procedimento, os instrumentos de recolha e as técnicas de tratamento de dados.

Atento à revisão da literatura, realizaram-se sete entrevistas exploratórias com um único guião, pelas áreas do conhecimento previamente identificadas e também consideradas conceitos estruturantes. Contemplaram-se as dimensões sociodemográficas operacional e académica. Estas entrevistas permitiram construir a problemática e retificaram o campo de investigação, obtendo-se também pistas com vista a referenciar as entidades para as entrevistas semiestruturadas de aprofundamento subsequentes.

Nas 13 entrevistas semiestruturadas de confirmação, as áreas de conhecimento e os conceitos estruturantes mantiveram-se, mas alargaram-se as dimensões sociodemográficas à política e à estratégia.

Recorreu-se também à *elite interviewing*, para atingir a clarificação pretendida e identificar os pontos de saturação. Conforme Johnson e Reynolds (2005, p. 271), não sendo uma entrevista estandardizada, insta a uma personalização considerando o conhecimento, as funções e a experiência específicas do entrevistado. Como tal, foram aplicados quatro guiões-tipo distintos.

As entrevistas exploratórias foram realizadas de 4 a 17 de novembro de 2020, tendo sido contemplados os perfis e as dimensões sociodemográficas.

Apresentam-se no Quadro 2 as frequências e as respetivas percentagens das respostas por cada uma das áreas do conhecimento e das dimensões sociodemográficas, bem como, as abarcadas em simultâneo, nos respetivos contextos.

Quadro 2 – Entrevistas exploratórias: áreas do conhecimento e dimensões sociodemográficas

ÁREAS DO CONHECIMENTO CONCEITOS ESTRUTURANTES						DIMENSÕES SOCIODEMOGRÁFICAS			
FP	IA	SIG	3 ÁREAS	2 ÁREAS	1 ÁREA	OP[20]	AC[21]	2 DIM[22]	1 DIM
5 71%	7 100%	6 85%	5 71%	1 14%	1 14%	6 85%	4 57%	3 42%	4 57%

As entrevistas semiestruturadas foram realizadas entre os dias 26 de fevereiro e 26 de março 2021.

Tabela 1 – Lista dos entrevistados

Entidade	Função
Antero Luís	Secretário de Estado Adjunto e da Administração Interna
Helena Fazenda	Secretária-Geral do Sistema de SI
Nelson Lourenço	Presidente do Grupo de Reflexão Estratégica sobre Segurança; Professor Universitário
José Magalhães	Deputado à Assembleia da República; Professor Universitário
Arlindo Oliveira	Professor do Instituto Superior Técnico (IST); Presidente do Instituto de Engenharia de Sistemas e Computadores, Investigação e Desenvolvimento; Membro do Conselho de Administração da Caixa Geral de Depósitos
Carlos Caleiro	Professor do IST, Departamento de Matemática; Investigador do *Security and Quantum Information Group* (SQIG) -Instituto de Telecomunicações
Miguel Pupo Correia	Professor do IST, Departamento de Engenharia Informática
Marco Painho	Professor Catedrático da Professor da *NOVA Information Management School*
Eduardo Magrani	Advogado, Professor Universitário e Pesquisador – Brasil
José Guilherme; COR	Diretor da Direção de Comunicações e Sistemas de Informação da GNR
José Moisés; COR	Diretor da Direção de Informações da GNR
João Nortadas, COR	Diretor da Direção de Investigação Criminal da GNR
José Leonardo, superintendente	Diretor do Departamento de Sistemas de Informação e Comunicações da PSP

Foi realizada uma recolha direta da informação bibliográfica geral e específica, com origem em fontes diversas (Sarmento, 2013, pp. 18-21).

Acresce referir que a realização das sete entrevistas exploratórias e a participação em seis seminários internacionais e *workshops* (ESRI EUE The Science of where; ENISA (European Union Agency for Cybersecurity): Anual privacy forum (APF) 2020 - ENISA, DG CONNECT and the Catholic University of Portugal, Lisbon School of Law; Portugal Digital Summit; ILEAnet Public Workshop 3 on Innovative Technologies for Border Management; Microsoft Security & Compliance Summit: Europe; Microsoft Security & Compliance Summit: Europe) e a consequente convergência da recolha e da análise destes elementos permitiu identificar não só as fontes primárias, as fontes secundárias e os normativos legais aplicáveis, como também fixar as três dimensões do conhecimento exploradas: a FP, a IA e os SIG.

Posteriormente, pela observação não participante foi obtida informação qualitativa, através da realização de entrevistas semiestruturadas e de *elite*, com o objetivo de certificar e complementar a recolha documental, por um lado, e de avaliar os indicadores dos conceitos identificados, por outro (Santos & Lima, 2019, p. 94).

Nas entrevistas semiestruturadas foi aplicada análise de conteúdo, considerando a: validade; relevância; especificidade e clareza; profundidade e extensão (Sarmento, 2013, pp. 51-52).

Os dados foram categorizados considerando as dimensões e os respetivos indicadores do modelo de análise. Tendo-se identificado as: unidades de registo; unidades de contexto e unidades de enumeração ou contagem, necessárias à identificação de segmentos de resposta e à construção das matrizes de análise de conteúdo (Sarmento, 2013, pp. 53-54).

Como resultado, foi criada uma matriz resumo de análise de conteúdo de todas as entrevistas (Bardin, 1977, pp. 36-46), a partir da qual se apresentam os resultados consolidados para complemento das respostas às questões de investigação.

4. APRESENTAÇÃO DOS DADOS E DISCUSSÃO DOS RESULTADOS

No presente capítulo apresentam-se os dados com base na profundidade da pesquisa e no trabalho de campo, discutindo-se também os resultados alcançados com a objetividade da análise metodológica.

Assume-se analisar teorias em confronto, exaltar inquietações e identificar perspetivas de futuro desenvolvimento desta temática candente.

4.1. Áreas de aplicação da Inteligência Artificial à atividade operacional das Forças e Serviços de Segurança

Em termos de aplicação às FSS, advoga-se que a IA pode ser utilizada em diversas áreas, agregando-se globalmente: nas vigilâncias; na capacidade de recolha e análise de grandes volumes de dados e numa análise e avaliação de risco mais refinada e precisa.

Como exemplos mais específicos apresentam-se: o reconhecimento de imagem, inclusive com deteção da expressão facial; a identificação de emoções; o reconhecimento de voz e de comportamentos suspeitos relativos a alterações de ordem pública; a pesquisa de pessoas desaparecidas; a monitorização das redes sociais; a utilização dos drones; a robotização com vista ao controlo e identificação de objetos ou pessoas; a definição de perfis criminais e a análise e controlo da sinistralidade rodoviária.

Todas estas aplicações têm vindo a ser, cada vez mais, desenvolvidas pela utilização de algoritmos empregues na AM e na aprendizagem profunda[20], proporcionando-se às FSS a transição de um policiamento de cariz mais reativo para os modelos de policiamento mais proativos, de que se destaca o PP. Também Walch (2020) reporta que a AI é essencial para a FP, podendo ser utilizada em diversas áreas, com aumentos de eficiência, com mais expressão na videovigilância analítica de pessoas e de situações anómalas.

A IA serve, inclusive, para modelar: os atos criminosos; o comportamento e o modo de raciocínio do criminoso; bem como o comportamento e o raciocínio do investigador (Perrot, 2017, p. 72 e 73).

P. Perrot (entrevista por *email*, 08 de novembro de 2020) também considera que a IA pode ser aplicada nos diferentes níveis: estratégico, operacional e tático.

Pela natureza altamente dinâmica do desenvolvimento destas tecnologias aplicadas à FP, este é ainda um processo em construção (Perrot, 2017, p. 75), mas permite, desde já, assumir-se que *alavancam o produto operacional* e, consequentemente, a cabal e judiciosa utilização de recursos.

---

[20] Tradução do Autor de "*deep learning*". Cfr. o conceito no Apêndice A.

4.1.1. A prevenção e a investigação criminais

Cusson e Lemieux (2007, p. 404) considera que a prevenção criminal compreende todas as ações não coercivas relativas às causas, aos motivos e aos preliminares da criminalidade, a fim de reduzir a probabilidade da sua ocorrência ou da sua gravidade.

Tal como preconizado no art.º 1.º da *Lei de Organização da Investigação Criminal*, aprovada pela Lei n.º 49/ 2008, de 27 de agosto, a investigação criminal "compreende o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo."

Numa ótica garantística sobre eventuais abusos contra os direitos individuais no cumprimento desta atividade, Monte (2013, p. 91) observa que a atual codificação penal pode "considerar-se uma grande conquista da humanidade, pois que o indivíduo ganhou um estatuto de relevo, que passou a garantir-lhe protecção penal, incluindo e sobretudo, contra abusos do próprio Estado."

4.1.2. Policiamento preventivo e policiamento preditivo

Assume-se, genericamente, que ao policiamento preventivo cumpre antecipar os riscos de comportamentos desviantes, no limite, com contornos criminais.

Segundo Clemente (2015, p. 98), "[a] ação preventiva dos corpos policiais traduz-se em operações materiais de vigilância do domínio público". Também afirma que "a polícia privilegia a prevenção, logo, não se limita a repor a legalidade violada", devendo esta ação cumprir os limites da lei (Clemente, 2006, p. 36).

Na observância da prevenção, têm sido promovidas e desenvolvidas diversas metodologias de proatividade policial e de aproximação à comunidade, como forma de co-produção de segurança e de prognose do perigo.

Esta tipologia de policiamento coloca mais enfoque no planeamento de longo prazo do que o policiamento reativo, que assenta na resposta a incidentes e normalmente baseia-se em denúncias (Maguire, 2008, p. 437).

Hodiernamente, um dos modelos policiais proativos que pretensamente mais uso faz das TIC, inclusive da IA, é o PP. Este consiste no uso de dados históricos para criar previsões espácio-temporais de zonas de criminalidade ou pontos críticos, que permitirão uma tomada de decisão relativa ao balanceamento de recursos para os locais e momentos das ocorrências criminais (Ratcliffe, 2016, p. 151).

Este tipo de policiamento tem sido criticado porque coloca o enfoque na identificação de padrões de criminalidade e não nas suas causas, pelo que também se defende a sua complementaridade com iniciativas de prevenção situacional (McDaniel & Pease, 2021, p. 22), *i. e.*, relacionadas com as caraterísticas dos locais, como por exemplo: as condições de iluminação, a conceção urbanística sem becos ou que provoquem o isolamento e a estratificação social.

4.1.3. Síntese conclusiva e resposta à QD1

Tem-se vindo a observar uma alteração do paradigma nos modelos de policiamento, transitando-se do policiamento mais reativo para os modelos mais proativos, que fazem uso das TIC, *máxime* da IA, como é o PP.

Atento à questão: *Quais as áreas de aplicação da IA à atividade operacional das FSS?* Considerando a dimensão da *prevenção e investigação criminal e tendo como indicadores o policiamento preventivo, o PP e a análise e avaliação de risco*, os 13 entrevistados assumiram como mais expressivas na aplicação da IA à FP:

— *a análise e tratamento de grandes quantidades de dados ou metadados* (69%);

— *os sistemas para agregação e tratamento de vídeo proveniente de sistemas de videovigilância desenvolvidos internamente recorrendo à aplicação de aprendizagem de máquina* (53%);

— *a geração de indicadores preditivos com previsibilidade do surgimento de determinados fenómenos criminais — modelos preditivos de policiamento* (53%).

A *prevenção da criminalidade com maior eficiência* apenas foi referenciada por dois dos entrevistados (13%), assim como a *definição e avaliação de perfis de risco*.

Considerando as quatro dimensões sociodemográficas, pode-se concluir que são transversalmente mais valorizadas a análise de grandes volumes de dados, a videovigilância e a geração de indicadores preditivos, estando em linha com a revisão da literatura.

4.2. Limites éticos, legais e operacionais da aplicação da Inteligência Artificial pelas Forças de Segurança em Portugal

4.2.1. Direitos fundamentais: direito à privacidade

Villalon (1984, cit. Canotilho, 1991, p. 507) afirma que "onde não existir constituição não haverá direitos fundamentais (...). [Os] direitos fundamentais são-

no, enquanto tais, na medida em que encontram reconhecimento nas constituições e deste reconhecimento se derivem consequências jurídicas."

Por serem erroneamente considerados sinónimos, Canotilho (1991, p. 529) apresenta como diferenciação entre direitos do homem e direitos fundamentais: "*direitos do homem* são direitos válidos para todos os povos e em todos os tempos (...); direitos fundamentais são direitos do homem, jurídico-institucionalmente garantidos e limitados espacio- temporalmente, [*i. e.*, são] direitos objetivamente vigentes numa ordem jurídica concreta."

Os direitos fundamentais implicam que o Direito Constitucional zele pela proteção da pessoa humana, "são as posições jurídicas ativas das pessoas integradas no Estado-Sociedade, exercidas por contraposição ao Estado-Poder, positivadas no texto constitucional (...)" Gouveia (2013, p. 161).

Já Miranda (1998, p. 22) considera que "[tal] como o conceito de Constituição, o conceito de direitos fundamentais surge indissociável da ideia de Direito liberal", sendo que uma das suas caraterísticas é "o primado da liberdade, da segurança e da propriedade, complementadas pela resistência à opressão."

Na CRP, os direitos fundamentais encontram-se previstos na Parte I sob a epígrafe direitos e deveres fundamentais, congregando tanto os direitos, liberdades e garantias como os direitos e deveres económicos, sociais e culturais. No âmbito do estudo, referencia-se o art.º 27.º direito à liberdade e à segurança.

No tocante em específico ao *direito à privacidade*[21], o art.º 26.º *outros direitos pessoais* e o art.º 35.º *utilização da informátic*a, ambos da CRP, sendo direitos fundamentais, podem também constituir-se como um verdadeiro direito à privacidade no restante conjunto de direitos fundamentais relativos ao uso da informática aí contidos.

Neste seguimento, Gouveia considera que

> [a] observação dos direitos fundamentais à proteção dos dados pessoais informatizados em especial faz realçar a existência de quatro tipos de direitos: o direito ao controle dos dados pessoais informatizados [art.º 35.º, n.º 1, da CRP]; o direito a não difusão dos

[21] Acompanha-se Gouveia (2013, p. 924), ao assumir que a nossa constituição é uma referência quanto ao pioneirismo e qualidade conferida à proteção da "pessoa relativamente à utilização da informática". Também Castro (2005, p. 76) afirma que Portugal foi o "primeiro país a estabelecer constitucionalmente um direito fundamental à proteção de dados pessoais objeto de tratamento automatizado."

> dados pessoais informatizados [art.º 35.º, n.º 4, da CRP]; o direito à proibição do tratamento informatizado dos dados pessoalíssimos [art.º 35.º, n.º 3, da CRP] e a garantia da não atribuição de um número nacional único [art.º 35.º, n.º 5, da CRP]. (2013, p. 923)

Para Castro (2005, p. 76), este direito "permite que o indivíduo negue informação, se oponha à recolha, difusão, ou qualquer outro modo de tratamento, (...) preservando a sua própria identidade informática."

Tal como estabelecido no n.º 2, do art.º 35.º da CRP, garante-se a proteção dos dados pessoais através da Comissão Nacional de Proteção de Dados (CNPD), uma autoridade administrativa a funcionar junto da Assembleia da República[22].

Como instrumentos jurídicos para salvaguardar esta tutela, cumpre novamente referenciar a *Lei de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e a Lei de tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais*.

Em termos europeus, volta-se a aludir ao RGPD.

Cukier (2017, pp. 230-231) assume que a "diretiva de proteção de dados da [UE] [...] aponta para dar ao público o 'direito à explicação' para decisões algorítmicas, tal como tem o 'direito de ser esquecido' para a privacidade."

Tal como refere Castro (2005, pp. 85-92), atualmente, assistimos ao confronto entre dois valores constitucionais fundamentais: a segurança e a privacidade, em que "[as] comunicações eletrónicas aceleraram a transformação do indivíduo em pessoa electrónica, obrigada a viver num mundo de vidro."

Como remate, Magrani (2019, p. 264) considera que para se atingir "[...] uma regulação jurídica adequada e democraticamente legítima é importante debatermos as noções de privacidade, proteção de dados e ética que deverão nortear os avanços tecnológicos."

De uma forma global, apesar do PP conjugado com a IA ser uma vantagem relativa, nem sempre estas tecnologias correspondem à realidade, apresentam algumas fraquezas, alguns custos financeiros e comportam um *trade-off* entre a liberdade e a segurança (McDaniel & Pease, 2021, pp. i e xii).

Também não se podem descartar as dinâmicas de mercado relacionadas com a pressão de grandes gigantes tecnológicos em criar necessidades aquisitivas

---

[22] Cfr. CNPD (2020). [Página *online*]. Retirado de https://www.cnpd.pt

pelas FSS, inclusive de tentativas da inclusão de algumas soluções tecnológicas nas políticas públicas de segurança, o que poderá vir a criar um ambiente tóxico no seio da instituição policial. A título exemplificativo menciona-se o *PredPol* e o *Palantir*, nos EUA (McDaniel & Pease, 2021, p. xii).

4.2.2. Mecanismos de controlo e fiscalização internos e externos

Para controlar e fiscalizar as condutas desviantes, no caso particular dos militares da GNR, assume-se internamente a cadeia de Comando e a IG, que, como prescrito no art.º 27.º, n.º 1, da sua Lei Orgânica (LO), aprovada pela Lei n.º 63/2007, de 6 de Novembro, é responsável por desenvolver "acções inspectivas e de auditoria ao nível superior da Guarda, competindo-lhe apoiar o comandante-geral no exercício das suas funções de controlo e avaliação da actividade operacional (...), bem como no estudo e implementação de normas de qualidade."

Externamente, identifica-se a IGAI, que, *cfr*. estabelecido no art.º 2.º, n.º 1 da sua LO, aprovado pelo Decreto-Lei n.º 22/2021, de 15 de março, tem como missão: "assegurar as funções de auditoria, inspeção, controlo e fiscalização, de alto nível, relativamente a todas as entidades, serviços e organismos, dependentes ou cuja atividade é legalmente tutelada ou regulada pelo membro do Governo responsável pela área da administração interna."

Sem prejuízo dos mecanismos supramencionados, cumpre também identificar os Tribunais e a ainda a censura social, cada vez mais mediatizada.

4.2.3. Síntese conclusiva e resposta à QD2

Os limites da aplicação da IA pelas FS em Portugal percorrem as dimensões da legalidade constitucional e da legislação específica sobre proteção de dados, em linha com o enquadramento internacional, mormente o da UE. Ademais, no tocante aos limites éticos, existem no nosso país códigos deontológicos[23] da atividade policial e mecanismos de controlo e fiscalização internos e externos que também garantem o cabal comprometimento com os padrões internacionais. Relativamente aos limites operacionais, os mesmos prendem- se maioritariamente com: a aquisição das TIC; com as necessidades formativas específicas;

[23] Cfr. o conceito no Apêndice A.

com a cultura institucional mais ou menos permeável à sua adoção; com a anonimização dos dados e com a conceção de algoritmos que filtrem os enviesamentos e a discriminação.

Considerando a questão: *Quais os limites legais, éticos e operacionais da aplicação da IA pelas FS em Portugal?*

Pela análise das entrevistas, com fundamento na dimensão SI — *atividade operacional e nos indicadores: direitos fundamentais; direito à privacidade; códigos deontológicos e mecanismos de controlo e fiscalização internos e externos* foram identificados como segmentos mais expressivos:

— *devem ser cumpridos os princípios da necessidade, da proporcionalidade, segundo o axioma das potencialidades da tecnologia em prol da segurança dos cidadãos e prevenção da criminalidade* (53%);

— *devem existir mecanismos de auditoria internos e externos eficazes* (53%);

— *devem ser utilizadas considerando a observância da matéria sobre proteção de dados pessoais, designadamente a Lei n.º 58/2019 e a Lei n.º 59/2019 e outras leis conexas* (53%);

— *deve ser observado o direito à privacidade e à reserva da vida privada* (46%). Todos se encontram genericamente alinhados com a revisão da literatura específica, exceto o segmento: *estas tecnologias não devem promover a discriminação e a estigmatização, considerando o potencial enviesamento na conceção e na análise realizada pelos algoritmos* (23%). Atribui-se este baixo valor à necessidade de um conhecimento mais específico, apenas detido pela sensibilidade dos especialistas mais dedicados. Todos os outros segmentos menos cotados podem ser subsumidos pelos restantes, segundo a interpretação transmitida pelos entrevistados.

4.3 O papel dos Sistemas de Informação Geográfica para a construção de um mapa de risco da criminalidade na área de atuação da GNR, a partir de um Modelo de Risco do Terreno

4.3.1. Sistemas de Informação Geográfica e Modelos de Risco do Terreno

Os SIG, para além de outras funções, permitem exprimir graficamente concentrações de eventos criminais por camadas de espaço e tempo. As atuais capacidades analíticas de grandes volumes de dados, associadas à velocidade e à preditividade proporcionadas pela IA aplicada aos SIG, possibilitam ao decisor,

através de painéis de visualização, alocar recursos com melhor oportunidade e precisão na análise dos riscos e no combate a eventos futuros.

A preditividade aplicada pelos SIG tem ganho mais expressão nos MRT.

P. Perrot (*op. cit.*), considera que o MRT a aplicar é difícil de definir globalmente. Podem ser propostos diferentes modelos de cálculo de risco para conferir diferentes modalidades de ação ao nível da decisão.

4.3.2. Síntese conclusiva e resposta à QD3

Para resposta à QD *qual o impacto da integração da IA aplicada aos SIG na área de atuação da GNR?*, foram ainda consideradas como complementares as respostas às seguintes questões, realizadas apenas a cinco dos 13 entrevistados, atento ao respetivo perfil sociodemográfico específico:

— *Qual o papel dos SIG na construção de um mapa de risco da criminalidade nas áreas de atuação da GNR/ Polícia de Segurança Pública (PSP)?*

— *Quais os pressupostos necessários para a elaboração de um modelo concetual de risco do terreno para a construção de um mapa de risco do crime de roubo e do crime de furto em residência nas áreas de atuação da GNR/ PSP?*

— *Na elaboração dos Modelos de Risco do Terreno na GNR é utilizado algum software de cálculo de risco e de mapeamento da criminalidade, como por exemplo o RTMDx (Risk Terrain Modelling Diagnostics), da Universidade de Rutgers?*

Observando-se as dimensões *prevenção e investigação criminal e SI — atividade operacional; e os respetivos indicadores: sistemas de apoio à decisão e análise de informação criminal,* relevam-se com maior expressão os seguintes segmentos no conjunto das quatro questões:

— *garantia da fiabilidade dos dados inseridos* (80%);

— *permite ter um papel prospetivo em prol das operações* (60%);

— *têm um papel fundamental para refinar a preditividade* (60%).

Na QD específica, a que responderam a totalidade dos entrevistados, destaca-se:

— *melhor integração, análise e parametrização de grandes volumes de dados* (38%);

— *análise de segmentação para identificar padrões de criminalidade e visualizar estes padrões em mapas, para apoio tático às operações policiais (23%).*

As baixas percentagens reveladas nesta questão – entre 38% e 15% (com uma média de 18%), justificam-se pela especificidade da questão para oito

dos entrevistados, por um lado, e, relativamente aos restantes cinco, por terem respondido em associação com a questão n.º 4 — *como potenciar a IA aplicada aos SIG na GNR/ PSP, considerando o cálculo do risco das diferentes tipologias criminais?*

No restante, as respostas encontram-se alinhadas com a bibliografia analisada, sendo relevada a necessidade da fiabilidade dos dados e o seu contributo para a prospetiva e preditividade policial.

Também se assume que a GNR e a PSP *não utilizam especificamente o software RTMDx* (50%), adotando soluções diferenciadas entre si e entre as respetivas estruturas nacionais e distritais: *Na GNR utiliza-se o NUIX, o MS Power BI e o I2. Já na PSP, ao nível da Direção Nacional da PSP, é utilizado o MORE P e localmente as estruturas de investigação criminal utilizam algumas soluções diferenciadas* (50%).

De outra parte, releva-se de superior importância que ao nível da tutela se advogue uma plataforma comum às duas forças: "O Sistema de Informação Geográfica (SIG) do MAI pretende criar as condições para a disponibilização transversal de um Sistema sinérgico e com maior rentabilização de investimentos e custos para o MAI, denominado de GeoMAI" (A. Luís, entrevista por *email*, 01 de março de 2021).

4.4. A integração da Inteligência Artificial aplicada aos Sistemas de Informação Geográfica na GNR, considerando o cálculo de risco das diferentes tipologias criminais

Considerando a análise bibliográfica e as entrevistas exploratórias, foi possível constatar que no âmbito da *transformação digital da Guarda,* "o cerne de todo este processo transformativo será materializado através do SIIOP v3.0, com *dashboards* e capacidade de *Business Intelligence* associada à atividade operacional." (J. Nunes, op. cit.), estando neste momento a correr a v2.8.0.

Assim, projetam-se como desideratos institucionais "a utilização de ferramentas de *Business Intelligence*, criando as condições para que conceitos como *Intelligence-led Policing* e *Predictive Analysis* sejam utilizados pela Guarda no planeamento e orientação do esforço de policiamento" (J. Nunes, op. cit.).

Como horizontes temporais de concretização para o Sistema de *Business Intelligence Policial*, "estima-se que possa ser implementado até final de 2021". Já os conceitos de *Intelligence-led Policing* e *Predictive Analysis,* "a partir de 2022". Sendo também um desiderato a adoção do "*geoprofiling* em 2025" J. Nunes (op. cit.).

Já nas entrevistas semiestruturadas de confirmação, J. Guilherme (entrevista por *email*, 22 de fevereiro de 2021) considerou que os cenários operacionais do emprego da IA aos SIG na GNR, em específico, são:

— Análise de aglomerações – utilizar o SIG da GNR e informações provenientes dos módulos SIIOP e informação proveniente de sensores para identificar possíveis aglomerações de eventos ou pessoas.

— Predição de ocorrências – qual é o padrão do histórico de determinadas ocorrências (criminalidade, sinistralidade, fiscalizações, operações, etc.) e projetar qual será a tipologia das ocorrências esperadas para os próximos dias, tendo em conta fatores meteorológicos (...), efemérides de calendário ou efemérides diárias.

— *Dashboards* interativos — Relatórios dinâmicos e interativos contendo diferentes KPI's (*Key Performance Indicators*)[24], (...) para que sejam acedidas via *tablet/ smartphone* pelos militares da GNR que devam ter a necessidade de conhecer.

4.4.1. Síntese conclusiva e resposta à QC

Após o contributo da análise às questões anteriores, chega-se à construção da resposta à QC — *Como potenciar a IA aplicada aos SIG na área de atuação da GNR?*

Esta questão específica apenas foi colocada diretamente a cinco dos entrevistados, sendo que todos correspondem à dimensão sociométrica operacional e um deles acumula com a dimensão académica.

Foram consideradas as duas dimensões da análise: a prevenção e a investigação criminal e a SI — atividade operacional; e os correspondentes indicadores específicos desta questão em concreto: os sistemas de apoio à decisão e a análise de informação criminal.

Também foram contemplados os contributos de alguns dos indicadores e segmentos identificados relativamente às questões:

— Qual o impacto da integração da IA aplicada aos SIG na GNR/ PSP?

— Como potenciar a IA aplicada aos SIG na GNR/ PSP, considerando o cálculo de risco das diferentes tipologias criminais?

— Qual o papel dos SIG na construção de um mapa de risco da criminalidade nas áreas de atuação da GNR/ PSP?

[24] Tradução do autor: "indicadores chave de desempenho".

Como principais contributos foram identificados os segmentos: ter conhecimento das necessidades de informação para apoio à decisão (100%) e produção de relatórios dinâmicos e interativos contendo diferentes KPI's (40%).

Já no tocante às outras questões, releva-se: permite ter um papel prospetivo em prol das operações (60%); têm um papel fundamental para refinar a preditividade (60%) e melhor integração, análise e parametrização de grandes volumes de dados (38%).

Relativamente ao emprego da IA nas diversas aplicações policiais, P. Perrot (*op. cit.*) afirmou que mais importante do que a sua utilização, é saber qual a finalidade do seu emprego em concreto. Por vezes expressa-se a vontade sem antes identificar o propósito.

Considera-se que a aplicação de plataformas de MRT baseadas em IA, poderão vir a potenciar complementarmente os modelos de atuação policial utilizados na GNR, em geral e o cálculo de risco das diferentes tipologias criminais na sua área de atuação, em particular. Assim, advoga-se a prova de conceito do *software RTMDx*.

5. CONCLUSÕES

No presente estudo analisa-se a componente operacional da FP, considerando os atuais desenvolvimentos proporcionados pela adoção das TIC, de que se destacam as aplicações da IA a esta exigente atividade.

As TIC têm vindo a ser paulatina e transversalmente adotadas pela sociedade, em geral e pelas FSS, 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 C2, na gestão e balanceamento de recursos e na eficácia da deteção, no controlo e na irradicação 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.

Em particular, a utilização da IA aplicada aos SIG apresenta inegáveis vantagens competitivas, tendo em contraponto a imposição de limites de natureza legal, ética e operacional. Este é um caminho que está a ser trilhado na GNR com base na sustentabilidade, em paridade com objetivos de concretização no horizonte de 2025.

Como percurso metodológico e considerando o contexto do estudo, optou-se pela abordagem multidisciplinar, com recurso às metodologias das Ciências Sociais e Humanas e também às próprias da investigação jurídica e respetiva hermenêutica.

Como instrumentos de recolha, privilegiaram-se a análise documental e as entrevistas exploratórias, semiestruturadas e de *elite*, de confirmação, num total de 20, tendo sido consideradas no global as dimensões sociodemográficas política, estratégica, operacional e académica.

Assumiu-se uma posição filosófica ontológica construtivista e epistemológica interpretativista. Foi aplicado o processo e raciocínio indutivo e uma estratégia de investigação qualitativa, tendo como desenho de investigação o estudo de caso de um modelo concetual de cálculo de risco das diferentes tipologias criminais, através da aplicação da IA aos SIG pela GNR na sua área de atuação.

Atento o OE1 — *Analisar as áreas de aplicação da IA à atividade operacional das FSS* e a correspondente QD1, conclui-se que a IA pode ser utilizada em diversas áreas, agregando-se globalmente nas vigilâncias, na capacidade de recolha e análise de grandes volumes de dados e numa análise e avaliação do risco mais refinada e precisa.

Como exemplos concretos referem-se: o reconhecimento de imagem com deteção da expressão facial; o reconhecimento de voz; a identificação de emoções; o reconhecimento de comportamentos suspeitos; a pesquisa de pessoas desaparecidas; a monitorização das redes sociais; a utilização dos *drones*; a robotização; a definição de perfis criminais e a análise e controlo da sinistralidade rodoviária.

Para o universo dos entrevistados foram transversalmente mais valorizadas a análise de grandes volumes de dados, a videovigilância e a geração de indicadores preditivos.

No tocante ao OE2 — Distinguir os limites legais, éticos e operacionais da aplicação da IA pelas FS em Portugal, correspondente à QD2, considerando as três dimensões de limites: na dimensão legal, é possível concluir que deve existir um comprometimento com os direitos fundamentais constitucionalmente consagrados de que se destacam: o direito à liberdade e à segurança e o direito à privacidade; no tocante aos limites éticos, são relevados o Código Deontológico do Serviço Policial e os respetivos mecanismos internos e externos de controlo e fiscalização como são a IG da GNR e a IGAI; e, relativamente aos limites operacionais, destacam-se a aquisição das TIC, as necessidades formativas específicas, a cultura institucional

mais ou menos permeável à sua adoção, a necessidade de anonimização dos dados e a conceção de algoritmos que filtrem enviesamentos e discriminações.

Foi destacado pelos entrevistados que: devem ser cumpridos os princípios da necessidade e da proporcionalidade, segundo o axioma das potencialidades da tecnologia em prol da segurança dos cidadãos e da prevenção da criminalidade; devem existir mecanismos de auditoria internos e externos eficazes; a IA deve ser utilizada considerando a observância da matéria sobre proteção de dados pessoais e deve ser observado o direito à privacidade e à reserva da vida privada.

Relativamente ao OE3 — Analisar o papel dos SIG para a construção de um mapa do risco da criminalidade na área de atuação da GNR e à respetiva QD3, apurou-se que as atuais capacidades dos SIG, de que se destaca os MRT, permitem ao decisor alocar recursos com melhor oportunidade e precisão na análise dos riscos e consequentemente no combate a eventos criminais futuros.

Na opinião dos entrevistados foi considerado como mais relevante: garantir a fiabilidade dos dados inseridos; permitir ter um papel prospetivo em prol das operações e ter um papel fundamental para refinar a preditividade.

Adicionalmente foi também considerada: a melhor integração, análise e parametrização de grandes volumes de dados e a análise de segmentação para identificar padrões de criminalidade e visualizar estes padrões em mapas, para apoio tático às operações policiais.

Cumpre também relevar que ao nível do MAI foi apontado o caminho para uma plataforma comum à GNR e à PSP.

Quanto ao OG — Analisar o impacto da integração da IA aplicada aos SIG na GNR, intimamente relacionado com a QC — Como potenciar a IA aplicada aos SIG na área de atuação da GNR?, verifica-se que da conjugação da análise bibliográfica e da construção das respostas às QD, se salienta que a incorporação alargada da IA nos SIG da GNR irá capacitar a instituição para uma melhor preditividade operacional, a par de uma superior capacidade de C2 e de um balanceamento de recursos mais judicioso, segundo critérios de evidência científica. Será possível uma maior velocidade e capacidade analítica de grandes volumes de dados, por forma a identificar concentrações de diversas tipologias criminais, fazer a sua análise e avaliação do risco e consequentemente projetar melhores respostas no tempo e no espaço.

Foram identificados pelos entrevistados como melhor forma de potenciar a IA aos SIG: ter conhecimento das necessidades de informação para apoio à decisão

e a produção de relatórios dinâmicos e interativos contendo diferentes indicadores chave de desempenho.

Também foi salientado que: permitem ter um papel prospetivo em prol das operações e têm um papel fundamental para refinar a preditividade e melhor integração, análise e parametrização de grandes volumes de dados.

Como contributos para o conhecimento identificam-se: o levantamento atualizado do estado da arte específico de uma área em desenvolvimento acelerado e de constante inovação, como é a IA e a sua aplicação aos SIG e ainda o diagnóstico realizado aos SIG no tocante à prevenção e ao combate à criminalidade, tanto na GNR, como na PSP, ainda que de forma mais limitada. Também se apresentam os anseios da GNR relativamente a esta capacidade e as mais valias da sua adoção generalizada no futuro.

Como limitações da investigação, aponta-se o período pandémico que atravessamos e que, neste particular, compromete as entrevistas presenciais e a visita a alguns locais para assistir à aplicação real dos SIG.

Como estudo a desenvolver, que se observa complementar a este, propõe-se identificar especificamente os impactos da implementação transversal da plataforma SIG GeoMAI.

Como recomendação, sugere-se promover formação alargada em SIG a todas as Secções de Investigação Criminal do dispositivo da GNR, mormente na área de análise de informação, a par da adoção de uma plataforma SIG única para utilização transversal em toda a instituição.

Como consideração de ordem prática, propõe-se desenvolver um projeto piloto num Comando Territorial da GNR em que seja utilizada uma plataforma de MRT, por forma a aferir as reais potencialidades da sua aplicação institucional e eventual aplicação generalizada a todo o território nacional, sugerindo-se a prova de conceito do *software RTMDx*.

Em suma, considera-se que a aplicação da IA aos SIG na GNR deverá continuar a fazer parte da sua estratégia de desenvolvimento tecnológico, permitindo, assim, uma mais eficiente prevenção e combate à criminalidade e, em simultâneo, uma judiciosa alocação de recursos, segundo critérios de oportunidade e de boa gestão.

Advoga-se que os pressupostos da inovação e do conhecimento devem nortear a atividade desenvolvida pela GNR e que, mais do que transversais à estrutura institucional e aos respetivos processos, devem ser transferíveis para os seus militares no terreno. Por fim, na *economia desta equação,* assume-se que o desenvolvimento tecnológico nunca deverá descorar a humanização da FP.

REFERÊNCIAS BIBLIOGRÁFICAS

Alexandre, S. (2014). SIG — Modelos de análise preventiva e preditiva de fenómenos criminais (Crime Mapping e Geoprofiling). *Pela Lei e Pela Grei – Revista da Guarda Nacional Republicana,* 33–37.

Amaro, A. (2012). *O Socorro Em Portugal*. Lisboa: FCT.

Amorim, M. A. (2019). *A GNR e o Novo Quadro Financeiro Plurianual da União Europeia: Oportunidades e Desafios* (Trabalho de Investigação individual do Curso de Estado- Maior Conjunto 2018/2019). Instituto Universitário Militar [IUM], Lisboa.

Andrade, J. C. V. de. (2012). *Os Direitos Fundamentais na Constituição de 1976*. Coimbra: Almedina.

Andrade, J., Lobo, V., Morgado, J., Santos, L. & Silva, N. (2017). O reconhecimento formal da área científica das ciências miliares: um imperativo e uma inevitabilidade? *Revista Militar*, 2583, 2-20.

Anyinam, C. (2015). Using risk terrain modeling technique to identify places with the greatest risk for violent crimes in New Haven. Em *Crime Mapping & Analysis News,* 26–32. USA: A police foundation publication.

Ascensão, O. (1991). *O Direito — Introdução e teoria geral* (6.a Ed). Coimbra: Almedina.

Avent (2017). O grande desafio da inovação. Em: *Megatech – As grandes inovações do futuro*, 106–21. Lisboa: Clube do Autor.

Bardin, L. (1977). *Análise de Conteúdo*. Lisboa: Edições 70.

Bryman, A. (2012). *Social Research Methods* (4.ª Ed.) Oxford: Oxford University Press.

Brynjolfsson, E., & McAfee, A. (2020). O negócio da inteligência artificial. Em *Inteligência atificial. Harvard Business Review*, 19 – 38. Coimbra: Actual.

Cabral, P., Ribeiro, Pereira, J. & Painho, M. (2018). Análise espacial avançada no contexto da segurança interna. Em *Modelos Preditivos e Segurança Pública,* 231–51. Porto: Fronteira do Caos.

Caetano, M. (2008). *Manual de Direito Administrativo*. (Vol. II. 10.ª Ed.). Coimbra: Almedina.

Campbell, T. (2018). Opportunities and Challenges from Artificial Intelligence for Law Enforcement. [Online]. Retirado de https://www.futuregrasp.com/opportunities-from-artificial-intelligence-for-law- enforcement

Canas, V. (2007). A Actividade de Polícia e a Proibição do Excesso: as Forças e Serviços de Segurança em Particular. Em *Estudos de Direito e Segurança*. Vol. I., 445 a 481. Coimbra: Almedina.

Canotilho, G. (1991). *Direito Constitucional* (5.a Ed.). Coimbra: Almedina.

Caplan, J. (2014). Risk Terrain Modeling for Strategic and Tactical Action. Em *Crime Mapping & Analysis News* (Issue I). USA: A police foundation publication.

Caplan, M. & Kennedy, L., Eds. (2011). *Risk Terrain Modeling Compendium*. New Jersey: Rutgers Center on Public Security.

Castro, C. (2003). *A questão das polícias municipais*. Coimbra: Coimbra Editora.

Castro, C. S. (2005). O Direito à autodeterminação informativa e os novos desafios gerados pelo direito à liberdade e à segurança após o 11 de Setembro. Em *Estudos em Homenagem ao Conselheiro José Manuel Cardoso da Costa*. Vol. II. Coimbra: Coimbra Editora.

Clemente, P. (2006). *A polícia em Portugal*. Lisboa: INA.

Clemente, P. (2015). *Cidadania, Polícia e Segurança*. Lisboa: Instituto Superior de Ciências Policiais e Segurança Interna.

Comissão Europeia (2018). Inteligência artificial para a Europa [Online]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM%3A2018%3A237%3AFIN

Comissão Europeia (2020). *Livro branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança* [versão PDF]. Retirado de https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial- intelligence-feb2020_pt.pdf

Comissão Europeia (2021). High-level expert group on artificial intelligence. [Online]. Retirado de https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai Comissão Nacional de Proteção de Dados (2020). [Página *online*]. Retirado de https://www.cnpd.pt

Cusson, M., Dupond, B. & Lemieux, F. (2007). *Traité de Sécurité Intériere* (1.ª Ed.) Montreal: Presses Polytechnique et Universitaires romandes.

Decreto-Lei n.º 22/2021, de 15 de março (2021). *Orgânica da Inspeção-Geral da Administração Interna*. Diário da República, 1.ª série, n.º 51, 34-40. Lisboa: Governo.

Decreto-Lei n.º 249/2015, de 28 de outubro (2015). *Aprova a orgânica do ensino superior militar, consagrando as suas especificidades no contexto do ensino superior, e aprova o Estatuto do Instituto Universitário Militar. Diário da República* 1.ª série — N.º 211. Lisboa: Ministério da Defesa Nacional.

Decreto-Lei n.º 47344, de 25 de novembro (1966). *Código Civil. Diário do Governo* n.º 274/1966, Série I. Lisboa: Governo.

Decreto-Lei n.º 48/1995, de 15 de março (1995). *Aprova o Código Penal. Diário da República* n.º 63/ 1995, Série I-A. Lisboa: Governo.

Decreto-Lei n.º 78/1987, de 17 de fevereiro (1995). *Aprova o Código do Processo Penal. Diário da República* n.º 40/1987, Série I. Lisboa: Governo.

Dias, G. (2006). Segurança Interna. Em *II Colóquio de Segurança Interna – ISCSPI,* 340. Coimbra: Almedina.

Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril (2016). *Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119/89. Bruxelas: UE.

Domingos, P. (2017). *A revolução do algoritmo mestre*. Barcarena: Manuscrito.

Duque, R. (2015). Singularidade da coexistência da liberdade e da segurança em democracia, 55-69. Em *Liberdade e Segurança*. Lisboa. ISCPSI.

Fernandes, F. (2021). *Inteligência Artificial, Segurança e Direitos* (Tese de Dissertação de Mestrado em Segurança da Informação e Direito do Ciberespaço). Instituto Superior Técnico [IST], Lisboa.

Fernandes, L. F. (2020). Inteligência Artificial – desafios e oportunidades para a polícia. *Polícia Portuguesa*, V Série, n.º 2, julho – setembro, 30-35.

Ferreira, J. & Martins, J. (2011). A geografia da criminalidade. Em *Geografia ativa* [versão PDF], 613-619. Retirado de http://dx.doi.org/10.14195/978-989-26-0244- 8_69.

Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. *Harvard Data Science Review,* Issue 1.1. Retirado de https://doi.org/10.1162/99608f92.8cd550d1

Fontes, J. (2015). A superioridade ética do Estado. Em *Liberdade e segurança*, 39-53. Lisboa: ISCPSI.

Freixo, Manuel. (2009). *Metodologia Científica: Fundamentos, Métodos e Técnicas*. Instituto Piaget.

GNR (1996). *Manual de Operações Volume I*. Vol. I. Lisboa: Comando Geral da GNR.

GNR (2020). A Estratégia da Guarda 2025 (EG2025), Uma Estratégia centrada nas Pessoas. Lisboa: GNR.

Gonçalves, M. (2020). *Crime mapping e os sistemas de informação geográfica (*Tese de Dissertação de Mestrado em Ciências Militares, Segurança). Academia Militar [AM], Amadora.

Gouveia, J. (2013). *Manual de Direito Constitucional*. Vol. I e II. (5.ª ed.). Coimbra: Almedina.

Gouveia, J. (2014). *Leis de Direito e da Segurança*. Lisboa: Quid Juris.

Harries, K. (1999). *Mapping Crime: Principle and Practice*. Washington, DC: National Institute of Justice.

Hassemer, W. (1995). História das ideias penais na Alemanha do pós-guerra. Em *Segurança Pública no Estado de Direito*. Lisboa: AAFDL.

Huxley, A. (2013). *Admirável Mundo Novo*. Lisboa: Antígona.

IPQ, (2011). *ISO Guia 73 – Gestão do risco – Vocabulário*. Caparica: IPQ.

João, P., Lobo, V. & Bação, F. (2013). Modelo Preditivo da Criminalidade». Em *Como tornar Portugal um País seguro?* N.o 2. Vol. 2.o, 139 a 182. Lisboa: Bnomics.

Johnson & Reynolds (2005). *Policy Research Methods*. California: CQ Press.

Johnson, S. (2017). Crime Mapping and Spatial Analysis. Em *Environmental criminology and crime analysis*, 199 – 223. New York: Routledge.

Lei n.º 1/1976, de 10 de abril (1976). *Constituição da República Portuguesa*. *Diário da República* n.º 86/1976, Série I. Lisboa: Assembleia da República.

Lei n.º 45/2019, de 27 de junho (2019). *Revisão global da linguagem utilizada nas convenções internacionais relevantes em matéria de direitos humanos a que a República Portuguesa se encontra vinculada*. *Diário da República*, 1.a série – N.º 121. Lisboa: Assembleia da República.

Lei n.º 49/2008, de 27 de agosto (2008). *Aprova a Lei de Organização da Investigação Criminal*. *Diário da República* n.º 165/2008, Série I. Lisboa. Assembleia da República.

Lei n.º 53/2008, de 29 de agosto (2008). *Lei de Segurança. Interna*. *Diário da República*, I Série, 167, 6135-6141. Lisboa: Assembleia da República.

Lei n.º 58/2019, de 8 de agosto (2019). *Lei de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. *Diário da República* n.º 151, 1.ª série. Lisboa: Assembleia da República.

Lei n.º 59/2019, de 8 de agosto (2019). *Lei de tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais*. *Diário da República* n.º 151, 1.ª série. Lisboa: Assembleia da República.

Lei n.º 63/2007, de 6 de novembro (2007). *Orgânica da Guarda Nacional Republicana*. *Diário da República*, 1.a série — n.º 213. Lisboa: Assembleia da República.

Magrani, E. (2018). Governance of internet of things and ethics of artificial intelligence. [Online]. Retirado de https://medium.com/@eduardomagrani/governance-of-internet-of-things-and-ethics-of-intelligent-algorithms-adabc1074204

Magrani, E. (2019). *Entre dados e robôs — ética e privacidade na era da hiperconectividade* (2.ª Ed.). Porto Alegre: Arquipélago Editorial.

Maguire, M. (2008). Criminal investigation and crime control. Em *Handbook of Policing*, 430–64. New York: Routledge.

McDaniel, J.L.M., & Pease, K.G. (Ed.). (2021). *Predictive Policing and Artificial Intelligence* (1.ª Ed.). New York: Routledge.

Miranda, J. (1988). *Manual de Direito Constitucional — Direitos Fundamentais*. Vol. IV. Coimbra: Coimbra Editora.

Monte, M. (2013). Direito Penal da Sustentabilidade? Tópicos para um novo paradigma na tutela penal do ambiente. *Jurismat*, n.º 3, 91-101. ISSN: 2182-6900.

Neto, M., Ribeiro, S., Motta, M. & Sarmento, P. (2018). Implementação de um dashboard para visualização e análise de dados de segurança. Em *Modelos Preditivos e Segurança Pública,* 157 – 208. Porto: Fronteira do Caos.

Nogueira, J. (2005). *Pensar a Segurança e a Defesa*. Lisboa: Edições Cosmos e Instituto de Defesa Nacional.

Oliveira, A. (2018). Público online. *A Singularidade Tecnológica*. Retirado de https://www.publico.pt/2018/10/12/opiniao/opiniao/a-singularidade-tecnologica-1847173

Parlamento Europeu (2021). O que é a inteligência artificial e como funciona? [Online]. Retiradode https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona

Pereira, R. (2007). *Conciliação entre liberdade, segurança e justiça em Portugal. Paper apresentado no Seminário Liberdade, Segurança e Justiça: Valores Fundamentais da Europa*. Lisboa.

Perrot, P. (2017). What about AI in Criminal Intelligence? From Predictive Policing to AI Perspectives. Em *European Police Science and Research Bulletin*, 65-76. UE 16.

Perry, W., McInnis, B., Price, C., Smith, S. & Hollywood., J. (2013). Predictive Policing — The Role of Crime Forecasting in Law Enforcement Operations. RAND.

Piza, E., Caplan, J. & Kennedy, L. (2011). Risk Clusters, Hotspots, and Spatial Intelligence: Risk Terrain Modeling as an Algorithm for Police Resource Allocation Strategies. *Journal of Quantitative Criminology - September 2010*. https://doi.org/10.1007/s10940-010- 9126-2

Raaijmakers, S. (2019). Artificial Intelligence for Law Enforcement: Challenges and Opportunities. *IEEE Security and Privacy*, 17(5), 74–77. https://doi.org/10.1109/MSEC.2019.2925649

Raposo, J, Gouveia, J. & F. P. Coutinho (2013). Polícia. Em *Enciclopédia da Constituição Portuguesa*, 282–84. Lisboa: Quid Juris.

Ratcliffe, J. (2016). *Intelligence-Led Policing*. New York, USA: Routledge.

Ratcliffe, J., Taylor, R., Askey, A. & Thomas, K. (2020). The Philadelphia predictive policing experiment. *Journal of Experimental Criminology*. https://doi.org/10.1007/s11292- 019-09400-2

Rego, A., Cunha, M., & Meyer Jr., V. (2019). Quantos participantes são necessários para um estudo qualitativo?. Linhas práticas de orientação. *Revista de Gestão dos Países de Língua Portuguesa*, 43-57. Retirado de http://bibliotecadigital.fgv.br/ojs/index.php/rgplp/article/view/78224/74934

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril (2016). *Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial da União Europeia, L 119/1. Bruxelas: UE.

Resolução 2016/C 202/02, de 7 de junho (2016). *Carta dos Direitos Fundamentais da União Europeia*. Bruxelas: Jornal Oficial da União Europeia.

Resolução do Conselho de Ministros (RCM) n.º 37/2002, de 7 de fevereiro (2002). *Código Deontológico do Serviço Policial*. *Diário da República* n.º 50/2002, Série I-B. Lisboa: Presidência do Conselho de Ministros.

Resolução n.º 217-A (III), de 10 de dezembro (1948). *Declaração Universal dos Direitos do Homem*. Nova Iorque: Assembleia Geral da Organização das Nações Unidas.

Ribeiro, S. (2018). Desafios da utilização de tecnologias de informação no apoio à tomada de decisão. Em *Modelos Preditivos e Segurança Pública*, 87–98. Porto: Fronteira do Caos.

Rodrigues, T., & Santos, A. (2018). Demografia política e políticas de segurança. Em *Modelos Preditivos e Segurança Pública*, 57–86. Porto: Fronteira do Caos.

Rosário, P. (2013). Direitos, liberdades e garantias. Em *Enciclopédia da Constituição,* 130–36. Lisboa: Quid Juris.

Sampaio, J. (2012). *O dever de protecção policial de direitos, liberdades e garantias*. Lisboa: Coimbra Editora.

Santos, L., & Lima, J. (Coords.) (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação*. Cadernos do IESM, 8. Lisboa: Instituto de Estudos Superiores Militares. Retirado de https://cidium.ium.pt/docs/publicacoes/CADERNO_8.pdf

Santos, R. (2013). *Crime analysis with crime mapping*. (3.ª Ed.). California: Sage Publications.

Santos, R. (2016). *Crime Analysis with Crime Mapping* (4.ª Ed.). Califórnia: Sage Publications.

Sarmento, M. (2013). *Metodologia Científica para a elaboração e apresentação de teses*. Lisboa: UAL.

Silva, N. (2010). *Cidadania e Segurança: Uma Análise Prospectiva*. *Paper* apresentado no I Congresso Nacional de Segurança e Defesa. Lisboa.

Silvério, P. (2020). *O planeamento operacional na GNR: como adaptar o planeamento OTAN à realidade nacional da GNR* (Trabalho de Investigação Individual do CPOG). Lisboa: IUM.

Sousa, M. & Galvão, S. (2000). *Introdução ao Estudo do Direito* (5.a Ed.). Lisboa: Lex. SSI. (2021). Relatório Anual de Segurança Interna (RASI) 2020. Lisboa: SSI.

Techaominuto (2021). Bruxelas propõe primeira lei europeia para inteligência artificial [Online]. Retirado de https://www.noticiasaominuto.com/tech/1730150/bruxelas-propoe-primeira-lei-europeia-para-inteligencia-artificial?utm_source=rss-tech&utm_medium=rss&utm_campaign=rssfeed

Valente, M. (2014). *Ciências Policiais — Ensaios*. Lisboa: Universidade Católica Editora.

Vilhena, M. (2019). *Modelo de risco de terreno: Uma estratégia preditiva para a implementação de sistemas de videovigilância* (Tese de Dissertação de mestrado em Ciências Policiais). Instituto Superior de Ciências Policiais e Segurança Interna [ISCPSI], Lisboa.

Walch, K. (2020). Forbes. *The Growth Of AI Adoption In Law Enforcement*. Retirado de https://www.forbes.com/sites/cognitiveworld/2019/07/26/the-growth-of-ai- adoption-in-law-enforcement/

Weisburd, D., Bernasco, W. & Bruinsma, G. (2009). *Putting crime in its place*. New York: Springer.

Wilson, R., & Filbert, K. (2017). Crime Mapping and Analysis. Em *Encyclopedia of GIS* (2.ª Ed.), 373 – 80, editado por S. Shekhar, Xiong, e X. Zhou. Springer.

APÊNDICE A – Quadro do corpo de conceitos auxiliares

Quadro 3 – Corpo de conceitos auxiliares

Conceito estruturante	Conceitos auxiliares
FP	Segurança Interna Conforme o plasmado no n.º 1 do art.º 1.º da atual LSI: A [SI] é a actividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática. Segundo Nogueira, a SI é: uma actividade plurisectorial, e que tem como domínios as informações, a manutenção da ordem pública, a prevenção geral da criminalidade, a coadjuvação na investigação criminal, e a protecção dos titulares dos órgãos de soberania, das instituições do Estado e dos serviços essenciais. (2005, p. 247)
	Forças e Serviços de Segurança Para a prossecução da atividade de SI o Estado português dispõe, além de outros instrumentos, das FSS, tal como preconizado no art.º 25.º, n.º 1 da LSI, "[as] forças e os serviços de segurança são organismos públicos, estão exclusivamente ao serviço do povo português, são rigorosamente apartidários e concorrem para garantir a [SI]." No mesmo diploma legal (art.º 25.º, n.º 2 da LSI) também se encontra prescrito que, do ponte de vista organizacional as FSS são: a GNR; a PSP; a Polícia Judiciária; o Serviço de Estrangeiros e Fronteiras e o Serviço de Informações de Segurança. Exercem ainda funções de segurança, os órgãos da Autoridade Marítima Nacional e do Sistema da Autoridade Aeronáutica (art.º 25.º, n.º 3 da LSI). Mas nem a CRP, nem a LSI estabelecem a distinção entre FS e Serviços de Segurança, essa distinção apenas é referida nas respetivas LO e na LO do MAI, sendo as dependentes do MAI a GNR e a PSP (art.º 6.º, n.º 2 da LSI). Neste particular, Canas (2007, p. 461) adota quatro critérios possíveis de distinção: o formal, o nominal, o estrutural e o material. Dias apresenta a seguinte distinção: As «forças de segurança» são organismos policiais armados e uniformizados, integrados por pessoal com o estatuto militar (GNR), com estatuto militarizado (PM), ou estatuto civil (PSP), mas sempre com estrutura organizativa caracterizada pela obediência à hierarquia de comando em todos os níveis. Os «serviços de segurança» são organismos públicos, integrados por agentes com estatuto análogo ao do pessoal da administração pública, hierarquicamente estruturados e institucionalmente vocacionados para o desempenho de atribuições específicas de natureza policial (PJ e SEF) ou no domínio das informações (SIS). (2006, p. 26)

[Cont.]

FP	Tipologias criminais As tipologias criminais no enquadramento jurídico nacional encontram-se previstas na Parte especial, no Livro II, do Código Penal, aprovado pelo Decreto-Lei n.º 48/95, de 15 de março. Assim, os crimes encontram-se agrupados por grandes tipologias criminais, nomeadamente: contra as pessoas, contra o património, contra a identidade cultural e integridade pessoal, contra a vida em sociedade, contra o Estado, contra animais de companhia e os crimes previstos em legislação avulsa. Considera-se também oportuno referenciar o Relatório Anual de SI como o documento de elaboração anual que se baseia na informação coligida e centralizada pela [Direção-Geral da Política de Justiça] a partir dos dados disponibilizados pelos [órgãos de polícia criminal], aos quais se aplicam técnicas e processos estatísticos (estratificação por forças de segurança, áreas de incidência e tipologias criminais), agregando resultados a partir da informação desagregada e de pormenor oriunda de cada um. Tal opção metodológica permite evidenciar o quadro de maturação ou evolução de grupos, tipologias criminais, medidas implementadas e respetivos resultados. (SSI, 2021, p. 4) Ainda relativamente à metodologia de elaboração do Relatório Anual de SI, a "análise dos dados foi realizada com base em *software* estatístico que insere os registos iniciais das ocorrências de crime entre 2019 e 2020. A informação geográfica, e a consequente produção de mapas temáticos, foi tratada por meio de um [SIG]" (SSI, 2021, p. 4).
	Direito à liberdade e à segurança Considerando o escopo do estudo, a FP como atividade, torna-se imprescindível abordar o enquadramento do artigo 27.º da CRP, sob a epígrafe direito à *liberdade e à segurança*. Avançando pelas ciências jurídicas, o direito à liberdade e segurança, encontra-se positivado nos mais elevados magistérios normativos internacionais e nacionais. "A relação simbiótica entre liberdade e segurança é bem exemplificada nas declarações de direitos que tendem, a agrupá-las num mesmo artigo" (Duque, 2015, p. 57). Assim, quanto ao quadro normativo internacional, apontamos a Declaração Universal dos Direitos Humanos, aprovada pela Resolução n.º 217-A (III), de 10 de dezembro (1948), tal como previsto no seu art.º 3.º, "todo o indivíduo tem direito à vida, à liberdade e à segurança pessoal". Na Carta dos Direitos Fundamentais da UE, aprovada pela Resolução 2016/C 202/02, de 7 de junho (2016), é consagrado no respetivo art.º 6.º – *direito à liberdade e à segurança*, no Título II – *liberdades*, que "[toda] a pessoa tem direito à liberdade e segurança". No ordenamento jurídico nacional, encontra-se previsto na CRP, onde se inserem os Direitos e Deveres Fundamentais, Título II da parte I — *Direitos, liberdades e garantias*, no Capítulo I – *Direitos, liberdades e garantias pessoais*. Assim, no n.º 1 do art.º 27.º, sob a epígrafe *direito à liberdade e à segurança*, estatui-se que "[todos] têm direito à liberdade e à segurança". Da análise do seu teor podemos afirmar "que existe uma relação de antinomia, e simultaneamente, de complementaridade entre os dois direitos" (Pereira, 2007), não sendo aceitável que um exista sem o outro. Esta norma encerra em si mesma o justo equilíbrio entre dois bens constitucionais fundamentais: a segurança, simultaneamente um dos fins do Estado, e a liberdade, de que os destinatários do mesmo não abdicam. O Tribunal Constitucional pronunciou-se neste sentido ao afirmar relativamente à *obrigatoriedade do porte de documento de identificação*, no Acórdão n.º 479/94, de 24 de agosto, que "a segurança tem que ser preservada por forma a que as pessoas possam viver em liberdade e segurança" (Sampaio, 2012, pp. 96-97).

[Cont.]

FP	Para Canas, numa perspetiva histórica, houve um tempo em que a segurança se sobrepunha sempre à liberdade. Houve outro em que, para certos sectores ideológicos, a segurança era vista como inimiga ou rival da liberdade, pelo que havia que preservar esta face àquela. Hoje sabe-se que não há liberdade sem segurança e é isso que a Constituição exprime quando fala da trilogia das funções da polícia: a defesa da legalidade, a garantia da segurança interna e a garantia dos direitos (da liberdade e outros) dos cidadãos. (…) À polícia a Constituição indica o caminho do equilíbrio entre segurança e liberdade. (2007, p. 455) Ainda assim, consideramos que este é um verdadeiro direito de *contexto*, pelo que a determinado momento poderá existir algum tipo de conflitos entre estes dois direitos com proteção constitucional. Um pode intersetar ou colidir com a esfera do outro, sendo que a sua hierarquização, em abstrato, é difícil de concretizar, pelo que, tal como refere Andrade (2012, pp. 299-303), pode adotar-se como regulador automático o *princípio da harmonização ou da concordância prática*, também presente na doutrina constitucional. Este exige necessidade e proporcionalidade na resolução do conflito, *i. e.*, "exige-se que o sacrifício de cada um dos valores constitucionais seja adequado à salvaguarda dos outros" e que se comprima, assim, o menos possível cada um dos valores em causa.
	Códigos deontológicos O Código Deontológico do Serviço Policial, RCM n.º 37/2002, de 7 de fevereiro, prescreve que este é "adoptado, no exercício de auto-regulação deontológica, pelos próprios agentes das forças de segurança." É também afirmado que os "padrões ético — profissionais de conduta, comuns a todos os agentes das forças de segurança, é, reconhecidamente, condição indispensável para um exercício credível e eficiente do serviço policial, enquanto parte integrante do Estado de direito democrático." Também no Manual de Operações da GNR, Volume I são apontados os princípios fundamentais do Código de Conduta da GNR, que, em paridade, também contribuem para enformar a sua matriz identitária e estatutária: — Cumprir a Missão de acordo com a causa Pública, o interesse Público e a Lei; — Servir a Colectividade Nacional e proteger todas as pessoas contra os actos ilegais; — Respeitar e proteger a dignidade humana; — Defender e proteger os direitos fundamentais de toda a pessoa; — Só aplicar a força em último caso e apenas na medida em que o cumprimento da sua missão o exigir; — Só recorrer às armas de fogo em legítima defesa, quando o presumido delinquente opuser resistência armada e se não for possível a utilização de outros meios; — Não divulgar informações de carácter confidencial, a não ser no cumprimento das suas funções ou quando as necessidades de justiça o exigirem; — Não infligir, instigar ou tolerar actos de tortura ou de qualquer outro tipo de castigo cruel, inumano ou degradante; — Não praticar o abuso de autoridade; — Combater e opor-se vigorosamente a todos os actos de corrupção. (1996, p. II-1), Adicionalmente, os militares e civis das FSS devem cumprir escrupulosamente o enquadramento jurídico nacional no tocante às medidas de polícia, às medidas especiais de polícia e às medidas cautelares e de polícia ínsitas na CRP, na legislação penal e na LSI, Lei n.º 1/1976, de 10 abril; Decreto-Lei n.º 48/95, de 15 de março; Decreto-Lei n.º 78/87, de 17 de fevereiro e Lei nº 53/ 2008, de 29 de agosto, respetivamente.

[Cont.]

IA	Dados No âmbito do estabelecido no art.º 3º, n. º 1, al. c) e o), do Regulamento de tratamento de dados pessoais, aprovada pela Lei n.º 59/2019, de 8 de agosto são: — «Dados pessoais», informações relativas a uma pessoa singular identificada ou identificável («titular dos dados»); — «Dados biométricos», dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitam ou confirmem a sua identificação única, tais como imagens faciais ou dados dactiloscópicos. Tal como previsto no art.º 4.º, n.º 1, do mesmo diploma, "[o] tratamento de dados pessoais deve processar-se no estrito respeito pelos direitos, liberdades e garantias das pessoas singulares, em especial pelo direito à proteção dos dados pessoais." Complementarmente, acompanhamos Castro quando revela o valor relativo dos dados: [a] navegação na *Internet*, o uso de correio eletrónico, a televisão interativa, os sistemas de localização, por permitirem o tratamento de gigantescas quantidades e qualidades de dados pessoais, comportam um especial grau de intrusão. Também por isso, o controle dos dados pessoais associados a estes meios é tão cobiçado pelos interesses económicos, bem como, no caso que agora mais nos importa, pelas polícias. (2005, p. 85) Tendo presente esta realidade, Avent (2017, p. 116) assume que "[os] governos estão a esforçar-se por estabelecer regras para a recolha e utilização de enormes quantidades de dados recolhidos de *smartphones* e outros dispositivos conectados – ao mesmo tempo que o público se mostra inquieto por o governo poder espiar esses dados."
	Algoritmos Segundo Domingos: Um algoritmo é uma sequência de instruções que diz a um computador o que fazer [...]. Os algoritmos evolutivos conseguem também fazer algo mais subtil: unir pontos entre acontecimentos que, individualmente, parecem inofensivos, mas que em conjunto constituem um padrão ameaçador. Esta abordagem poderia ter evitado o 11 de setembro. (2017, pp. 25-45)
	Aprendizagem de máquina Domingos considera que a AM assume muitas formas diferentes e é conhecida por muitos nomes diferentes: reconhecimento de padrões, modelação estatística, exploração de dados, descoberta de conhecimento, análise preditiva, ciência dos dados, sistemas adaptativos, sistemas auto-organizados, e muito mais. [...] Tecnicamente, a AM é um subcampo da IA [...] A AM é como ter um radar que vê o futuro. Não podemos apenas reagir às manobras do adversário: temos de as prever e evitar. (2017, pp. 32-45)
	Aprendizagem profunda Tal como clarifica Winblad é o ramo mais recente: os seus algoritmos são baseados em dados gerados pelas interações de múltiplas camadas de AM. O aumento exponencial dos dados digitalizados para alimentar sistemas de aprendizagem, os melhoramentos das ferramentas para os dados, o *software* essencial de fonte aberta e barata infraestrutura de nuvem conduziram a uma explosão de inovação na moderna IA. (2017, p. 99)

[Cont.]

SIG	Risco Um elemento estrutural da preditividade policial é a análise e a avaliação do risco, pelo que se considera oportuno definir estes conceitos. Conforme estabelecido pela *ISO Guia 73 — Gestão de risco – Vocabulário*, o risco é definido por "[efeito] da incerteza na consecução dos objectivos. (...) é frequentemente expresso como a combinação das consequências de um dado evento (incluindo alteração das circunstâncias) e a respectiva probabilidade de ocorrência" (IPQ, 2011, p. 6). Complementarmente, como afirma Amaro: > Os perigos são reais, mas os riscos são construções sociais. Por outro lado, as incertezas que são o que constitui um risco, podem tornar-se visíveis quando são socialmente definidas pelo conhecimento ou por formas de processamento de conhecimento como a ciência, o sistema legal e os media. (2012, p. 53)
	Análise e avaliação do risco Tal como estabelecido pela *ISO Guia 73 — Gestão de risco – Vocabulário*, a análise de risco é um "[processo] destinado a compreender a natureza de risco e a determinar o nível de risco. [Fornece] a base para a avaliação de risco e as decisões sobre o tratamento de risco" (IPQ, 2011, p. 12). Por sua vez, a *avaliação* de risco é um "[processo] de comparação dos resultados da análise de risco com os critérios de risco para determinar se o risco e/ou a respectiva magnitude é aceitável ou tolerável" (IPQ, 2011, p. 14).

ESTUDO 5 – PREVENÇÃO E ALERTA DA SINISTRALIDADE RODOVIÁRIA COM O CONTRIBUTO DA INTELIGÊNCIA ARTIFICIAL[1]

PREVENTING AND ALERTING ROAD ACCIDENTS WITH THE HELP OF ARTIFICIAL INTELLIGENCE

Pedro Miguel Monteiro Valente
Major de Infantaria da GNR

Paulo Infante
PhD, Docente na Unversidade de Évora

RESUMO

Na atualidade, a aplicação de sistemas baseados em inteligência artificial (IA) no combate à sinistralidade rodoviária já é uma realidade, apresentando resultados significativos. Em Portugal já foram dados os primeiros passos nesta área, principalmente através de projetos de investigação desenvolvidos por algumas Academias, dos quais se destaca o projeto da Universidade de Évora MOPREVIS. Partindo do argumento que a aplicação de metodologias de IA na construção de modelos preditivos potencia a prevenção e o alerta da sinistralidade rodoviária, afigurou-se pertinente analisar de que forma podem ser potenciados os contributos da IA no combate ao flagelo da sinistralidade rodoviária, usando como caso de estudo o modelo MOPREVIS. Para cumprir este desiderato, recorreu-se a um processo metodológico assente no raciocínio indutivo, materializado por uma estratégia de investigação mista, na qual se recorreu a técnicas de análise documental, inquéritos por entrevista e inquéritos por questionário, num desenho de pesquisa de estudo de caso. Foi possível concluir que a forma de potenciar os contributos da IA para a prevenção e alerta da sinistralidade rodoviária deve ser sustentada nas seguintes linhas de orientação estratégica: LOE1 - Assegurar qualidade e rigor; LOE2 - Automatizar; LOE3 - Desenvolver e diversificar; e LOE 4 - Cooperar e colaborar.

Palavras-chave: Alerta, inteligência artificial, MOPREVIS, prevenção, sinistralidade rodoviária

[1] Artigo adaptado a partir do Trabalho de Investigação Individual do Curso de Estado-Maior Conjunto (CEMC 2022-2023). A versão integral encontra-se disponível nos Repositórios Científicos de Acesso Aberto de Portugal (https://www.rcaap.pt/).

ABSTRACT

Currently, the application of artificial intelligence (AI) systems in combating road accidents is already a reality, with significant results. In Portugal, the first steps have already been taken in this area, mainly through research projects developed by some universities, including the MOPREVIS project at the University of Évora. Given that the application of AI methodologies in the construction of predictive models can enhance the prevention and alert of road accidents, it was pertinent to analyse how the contributions of AI can be enhanced in combating the scourge of road accidents, using the MOPREVIS model as a case study. To achieve this goal, a methodological process based on inductive reasoning was used, materialized by a mixed research strategy, which included techniques of documentary analysis, interview surveys, and questionnaire surveys in a case study research design. It was possible to conclude that the way to enhance the contributions of AI to the prevention and alert of road accidents should be based on the following strategic guidelines: LOE1 - Ensuring quality and rigor; LOE2 - Automating; LOE3 - Developing and diversifying; and LOE 4 - Cooperating and collaborating.

***Keywords**: Alert, Artificial Intelligence, MOPREVIS, Prevention Road Accidents*

1. INTRODUÇÃO

Atualmente, a segurança rodoviária é dos temas que mais preocupa a comunidade mundial (Organização Mundial de Saúde [OMS], 2021). As vítimas que resultam de sinistros rodoviários fazem da sinistralidade rodoviária um grave problema de saúde pública, sendo o sistema rodoviário considerado um dos mais complexos e perigosos com o qual as pessoas interagem diariamente (Leal, 2016). De facto, a OMS (2021) tem chamado a atenção para os milhões de vítimas que por ano morrem ou ficam com sequelas graves, decorrentes de sinistros rodoviários. De acordo com a referida organização, a sinistralidade rodoviária, a nível global e por ano, causa aproximadamente 1,3 milhões de mortes e 50 milhões de feridos, além de constituir a principal causa de morte de crianças e jovens adultos (entre os 5 e os 29 anos) em todo o mundo (OMS, 2021).

Todavia, este problema não se esgota na trágica perda de vidas humanas ou nos danos físicos e psicológicos irreparáveis que provoca nas vítimas e suas famílias. Ele dificulta e inibe também o desenvolvimento económico dos países. A sinistralidade rodoviária é um problema de saúde pública, mas também é um problema com impactos económicos e sociais, como refere o Plano Estratégico Nacional de Segurança Rodoviária 2020:

> Para além das perdas e do sofrimento humano (…) existe uma destruição de riqueza que, de acordo com valores do estudo para a Comissão Europeia anteriormente citado, terá ultrapassado em Portugal, nestes seis anos, os 12,4 mil milhões de euros. Destruição de riqueza que corresponde, numa média anual, a cerca de 1,24 % do PIB (Resolução do Conselho de Ministros n.º 85/2017, de 19 de junho, 2017).

Contudo, os perigos subjacentes à sinistralidade rodoviária podem ser prevenidos, ou pelo menos mitigados. A implementação de tecnologia e a adoção de políticas rodoviárias cada vez mais rígidas, têm obtido resultados positivos, que apesar de tudo ficam aquém das expetativas (Marcillo et al., 2022).

A utilização de sistemas baseados em inteligência artificial (IA), na área da segurança rodoviária, já é uma realidade, e tem apresentado resultados bastante significativos (Marcillo et al., 2022), nomeadamente no que respeita aos modelos preditivos da sinistralidade rodoviária, que garantem uma base cientificamente sólida no apoio à avaliação e seleção de medidas de segurança rodoviária e de apoio ao processo de tomada de decisão, apresentando custos bastante reduzidos (Yannis et al., 2016).

Em Portugal já foram dados os primeiros passos nesta área, principalmente através de projetos de investigação desenvolvidos por algumas Academias[2]. Dos diversos estudos em desenvolvimento, tem-se destacado o projeto da Universidade de Évora MOPREVIS[3] desenvolvido em parceria com o Comando Territorial (CTer) de Setúbal da Guarda Nacional Republicana (GNR). O objetivo final deste projeto foi construir uma ferramenta digital para apoiar a tomada de decisão em tempo real. Apesar de se encontrar ainda em fase experimental, este projeto apresenta um modelo bastante evoluído e consolidado, que aparenta possuir um elevado potencial de intervenção no combate à sinistralidade rodoviária, mas que se encontra limitado à zona de ação (ZA) do CTer de Setúbal da GNR.

---

[2] A título de exemplo, a Faculdade de Engenharia da Universidade do Porto promoveu alguns trabalhos de investigação nesta área em parceria coma concessionária Ascendi, designadamente com os seguintes temas: "Identificação e Análise de Fatores de Risco em Autoestrada: Aplicação de Modelos Estatísticos"; "Aplicação de Modelos de Previsão de Acidentes Rodoviários à Rede Ascendi".

[3] Moprevis - Modelação e predição de acidentes de viação (uevora.pt).

Perante este contexto, considera-se de extrema relevância analisar de que forma podem ser potenciados os contributos da IA para a prevenção e alerta da sinistralidade rodoviária, usando como caso de estudo o modelo MOPREVIS.

No atinente ao anteriormente exposto, a presente investigação tem como objeto de estudo a IA na Segurança Rodoviária, sendo delimitada em três domínios: no domínio temporal, espacial e de conteúdo (Santos & Lima, 2019). No que respeita ao domínio temporal, cinge-se ao período compreendido entre 2019, que corresponde ao início do projeto MOPREVIS, até 15 de abril de 2023, data após a qual não será possível incluir mais dados para a investigação. Quanto ao domínio espacial, o estudo está delimitado a Portugal continental. Em relação ao domínio do conteúdo, este trabalho limita-se aos contributos da IA para a segurança rodoviária.

Como objetivo geral (OG), partindo da tese que a aplicação de metodologias de IA na construção de modelos preditivos potencia a prevenção e o alerta da sinistralidade rodoviária, a presente investigação procura analisar de que forma podem ser potenciados os contributos da IA para a prevenção e alerta da sinistralidade rodoviária. Para a prossecução do cumprimento do OG e resposta à questão central (QC): de que forma podem ser potenciados os contributos da IA para a prevenção e alerta da sinistralidade rodoviária? propõem-se os seguintes objetivos específicos (OE): OE1. Analisar o enquadramento teórico da IA, no âmbito da prevenção e alerta da sinistralidade rodoviária; OE2. Caraterizar o projeto de Modelação e Predição de Acidentes de Viação no Distrito de Setúbal (MOPREVIS); OE3. Analisar as condições para aplicação do MOPREVIS a toda a ZA da Guarda Nacional Republicana (GNR).

A presente investigação contempla oito capítulos: no primeiro capítulo é feita a introdução da problemática e dos objetivos da investigação; no segundo capítulo é estabelecido o enquadramento concetual e metodológico; o terceiro capítulo alicerça a metodologia e o método da investigação; nos quarto, quinto e sexto capítulos são apresentados e analisados os dados recolhidos, procurando dar resposta às QD 1, 2 e 3 respetivamente; o sétimo capítulo reserva-se à análise SWOT[4], onde se materializa a resposta à QC; finalmente, o oitavo e último capítulo é relativo às conclusões.

[4] *Strength, Weakness, Opportunity, and Threat* (Humphrey, A., 2005)

2. ENQUADRAMENTO CONCEPTUAL E METODOLÓGICO

2.1. Prevenção

Segundo Bismael Moraes, a prevenção:

> Conduz a uma disposição preventiva, de aviso, precaução. Daí vem o adjetivo preventivo, mostrando o que é próprio para prevenir; e esse verbo prevenir é o mesmo que antecipar-se, chegar antes; tratar de evitar, acautelar-se, precaver-se; impedir que se execute ou que suceda. (Moraes, 2005, p. 50)

De acordo com Alves (2008, p. 133), "[…] é possível apontar quatro tipos de ações, bem caracterizadoras da atividade policial: as informações, a prevenção, a repressão e a assistência". Segundo o mesmo autor, a prevenção deve ser o objetivo principal da função polícia, a sua função primordial e a ela "deve corresponder o maior empenhamento, de modo que a função polícia produza a maior utilidade social" (Alves, 2008, p. 137). Acrescenta ainda que "a prevenção será conseguida - com base em informações, isto é, conhecimento do terreno e das ameaças, que permitam prever acontecimentos" (Alves, 2008, p. 134).

Já a prevenção no âmbito da segurança rodoviária, consiste na adoção de determinadas medidas criadas pelas várias entidades com responsabilidade na temática, tendo como fim último a prevenção de sinistros rodoviários e a redução das suas consequências (Racioppi, Eriksson, Tingvall, & Villaveces, 2004).

2.2. Alerta

Outro dos conceitos cuja definição importa abordar é a definição de alerta. A Estratégia Internacional das Nações Unidas para a Redução de Desastres define alerta ou o sistema de alerta como:

> o conjunto de capacidades necessárias para gerar e disseminar informações de alerta oportunas e significativas para permitir que indivíduos, comunidades e organizações ameaçadas por um perigo se preparem e ajam de forma adequada e em tempo suficiente para reduzir a possibilidade de dano ou perda. (UNISDR, 2009)

No que toca ao normativo legal português, podemos encontrar em diversos diplomas referências ao conceito de alerta, destacando-se o Decreto-Lei n.º 2/2019, de 11 de janeiro, que institui o Sistema Nacional de Monitorização e Comunicação de Risco, de Alerta Especial e de Aviso à População, que define o conceito como:

> […] a comunicação ao sistema de proteção civil da iminência ou ocorrência de um acidente grave ou catástrofe, acompanhada dos elementos de informação essenciais ao conhecimento da situação, de modo a permitir o desencadear de ações complementares no âmbito da proteção e socorro […]. (Decreto-Lei n.º 2/2019, de 11 de janeiro, 2019)

2.3. Sinistralidade rodoviária

O conceito de sinistralidade rodoviária parece estar perfeitamente assimilado pela sociedade, pois no que respeita a trabalhos académicos ou mesmo no quadro normativo legal não se observa em algum momento a preocupação no seu esclarecimento. Este facto pode indiciar que não se tem verificado algum tipo de enviesamento na sua interpretação. Todavia, dada a sua importância para a investigação, interpreta-se o conceito de sinistralidade rodoviária como o conjunto de ocorrências do sistema rodoviário nas quais surge um sinistro rodoviário.

Ainda respeitante a este conceito, importa referir que ao longo do estudo, tratando-se de um trabalho científico, é utilizada a expressão "sinistro rodoviário" e não "acidente rodoviário". A principal razão prende-se com a conotação de imprevisibilidade e aleatoriedade ligada ao termo acidente, ou seja, a eventos totalmente imprevisíveis (Pérez, 2011), pelo que é considerado que a semântica da palavra não coincide com o conceito atual. De acordo com o significado da palavra acidente, as únicas hipóteses de uso correto do termo são aquelas em que os eventos são conjuntamente imprevisíveis e inevitáveis (Tabasso, 2012). De facto, o estado atual do conhecimento científico e tecnológico da investigação de sinistros rodoviários permite quase banir a noção de imprevisibilidade, embora nem sempre a de inevitabilidade, pois trata-se de eventos passíveis de análise racional e ações corretivas. Por estas razões, o termo acidente rodoviário é usado exclusivamente para indicar eventos verdadeiramente imprevisíveis e inevitáveis e, por uma razão elementar de respeito intelectual, nas citações textuais dos autores que o usaram.

2.4. Inteligência artificial

De acordo com António Raimundo e Pedro Sebastião (2021, p. 7), em 1943 Warren McCulloch e Walter Pitts publicaram um artigo onde se referiam pela primeira vez ao termo "Redes Neuronais Artificiais" referindo tratar-se "[…] de

uma estrutura de representação e raciocínio artificiais que, através de um modelo matemático, poderiam realizar uma espécie de mímica do nosso sistema nervoso central". No entanto, acrescentam os autores, só em 1955 é que surge o termo "inteligência artificial" - da autoria do cientista John McCarthy, que a define como sendo "A ciência e a engenharia de fazer máquinas inteligentes, especialmente programas de computador inteligentes".

São inúmeras as definições de IA na atualidade. Segundo Carlos Alastruey (2021, p. 183) "é aquele ramo do conhecimento responsável por realizar processos computacionais capazes de realizar tarefas com base em duas características humanas fundamentais: o raciocínio e o comportamento". Para António Raimundo e Pedro Sebastião (2021, p. 6) a "A IA pode ser encarada como o desenvolvimento de "máquinas" que conseguem "pensar", aprender e adaptar " ou ainda a "Área que estuda o desenvolvimento de soluções digitais a aplicar em máquinas para realizarem atividades humanas de um modo autónomo" (2021, p. 38).

2.5. Modelação, *Machine Learning* e predição

Modelação estatística pode ser definida como um processo de tradução simplificada da realidade, onde se procura explicar e/ou predizer uma ou mais variáveis aleatórias de interesse com base em outras variáveis. Quando os analistas de dados aplicam vários modelos estatísticos aos dados que pretendem investigar, isso permite-lhes entender e interpretar as informações de forma mais clara e concisa. Em vez de filtrar os dados brutos, a modelação permite identificar relações entre variáveis, possibilitando a elaboração de previsões sobre conjuntos de dados (Stobierski, 2019).

Com o surgimento da IA, foi possível a aplicação de modelação estatística a conjuntos de dados imensamente superiores. Além do mais, possibilitou a aplicação de técnicas e algoritmos capazes de aprender de diferentes e novas formas de informação, construindo algoritmos que melhoram de forma autónoma com a experiência – atualmente designado por *Machine Learning*.

Segundo António Raimundo e Pedro Sebastião *Machine Learning* é:

> […] uma área que engloba os algoritmos e tecnologias aplicados em máquinas que, durante a conceção, foram desenvolvidas através de metodologias de "aprendizagem". Em vez de programar regras para que sejam executadas pela máquina, é possível que a máquina aprenda a "criar" essas regras a partir dos dados, chegando

> ao resultado esperado de uma forma autónoma. (Raimundo & Sebastião, 2021, p. 16)

O uso de novas fontes de informação bem como a aplicação de técnicas de algoritmos capazes de aprender - *Machine Learning* - possibilitou a obtenção de novos benefícios, designadamente a maior automatização dos processos de modelagem e autoaprendizagem, aumentando a capacidade preditiva dos modelos (Management Solutions, 2018).

Por sua vez a predição, ou seja, os modelos preditivos, possibilitam a correlação de informações de fontes heterogéneas (Marcillo et al., 2022, p. 2). Enquanto um Modelo Estatístico consiste no uso de estatísticas para construir uma representação dos dados e, em seguida, realizar uma análise que permita inferir relações entre variáveis e avaliar o seu efeito, um modelo de *Machine Learning* consiste na utilização de modelos matemáticos e estatísticos para obter uma compreensão geral dos dados e realizar previsões. Neste último, o computador é "ensinado a aprender", consegue entender padrões perante uma enorme quantidade de dados.

2.6. Modelo de análise

Com a realização das entrevistas exploratórias foram identificadas linhas orientadoras que permitiram a construção do modelo de análise, no Quadro 1, cujo intento é a estruturação de um quadro mental, fundamental para a sistematização dos objetivos, das questões, conceitos, dimensões, variáveis, bem como dos indicadores e das técnicas de recolha de dados selecionadas.

Quadro 1 – Modelo de análise

TEMA	**Prevenção e Alerta da Sinistralidade Rodoviária com o Contributo da Inteligência Artificial (IA).**						
TÍTULO	**Estudo de caso: A Modelação e Predição de Acidentes de Viação no Distrito de Setúbal (MOPREVIS).**						
TESE - ARGUMENTO	A aplicação de metodologias de IA na construção de modelos preditivos potencia a prevenção e o alerta da sinistralidade rodoviária.						
OBJETIVO GERAL	Analisar de que forma podem ser potenciados os contributos da IA para a prevenção e alerta da sinistralidade rodoviária.						
QUESTÃO CENTRAL	De que forma podem ser potenciados os contributos da IA para a prevenção e alerta da sinistralidade rodoviária?						
OBJETIVOS ESPECÍFICOS	**QUESTÕES DERIVADAS**	**CONCEITOS**	**DIMENSÕES**	**VARIÁVEIS**	**INDICADORES**	**Recolha de Dados**	
						Instrumentos	**Técnicas**
OE 1: Analisar o enquadramento teórico da IA, no âmbito da prevenção e alerta da sinistralidade rodoviária.	**QD1:** Quais os principais contributos teóricos da IA para a prevenção e o alerta da sinistralidade rodoviária?	- Prevenção - Alerta - Sinistralidade Rodoviária - Inteligência Artificial - Predição - Modelação	- Político-estratégica - Operacional - Tática	- Inteligência artificial - Sinistralidade Rodoviária	- Potencialidades - Vulnerabilidades - Ameaças - Oportunidades	- Entrevistas exploratórias - Entrevistas estruturadas - Questionários	- Análise documental - Análise de conteúdos - SWOT
OE 2: Caraterizar o projeto Modelação e Predição de Acidentes de Viação no Distrito de Setúbal (MOPREVIS).	**QD 2:** Quais as principais caraterísticas, potencialidades e limitações do projeto MOPREVIS?						
OE 3: Analisar as condições para aplicação do MOPREVIS a toda a zona de ação da Guarda Nacional republicana	**QD 3:** Quais as condições para aplicação do MOPREVIS a toda a zona de ação da Guarda Nacional Republicana?						

3. METODOLOGIA E MÉTODO

A investigação em apreço tem por base as normas em vigor no IUM, nomeadamente a NEP/INV-001(A1) e NEP/INV-003(A3), bem como as "Orientações Metodológicas para a elaboração de Trabalhos de Investigação", constantes do Caderno do IUM n.º 8, seguindo ainda a referenciação das Normas de Autor no IUM (Fachada, Ranhola, Marreiros, & Santos, 2020)

Considerando o objeto da presente investigação, foram adotadas opções metodológicas partindo-se de uma posição ontológica construtivista, tendo em conta "que os fenómenos sociais e os seus significados estão constantemente a ser executados pelos atores sociais" (Santos & Lima, 2019, p. 16), bem como uma abordagem epistemológica interpretativista, no sentido de compreender a realidade do objeto em estudo.

No que respeita ao raciocínio, a metodologia de investigação baseou-se no raciocínio indutivo, uma vez que teve como "ponto de partida a observação de factos particulares para, através da sua associação, estabelecer generalizações que permitam formular uma lei ou teoria" (Santos & Lima, 2019, p. 18). A investigação em apreço observou o caso particular do projeto MOPREVIS, através do qual se procurou ter uma perspetiva de uma dimensão transversal das potencialidade e contributos da IA para a prevenção e alerta da sinistralidade rodoviária.

Em relação à estratégia de investigação, face à natureza do objeto de estudo, adotou- se uma estratégia mista, combinando uma dimensão qualitativa, de cariz

preponderante, com reforço quantitativo, "de modo a capitalizar as potencialidades e a colmatar as vulnerabilidades de cada uma delas" (Santos & Lima, 2019, p. 29). No desenho de pesquisa utilizou-se o estudo de caso, considerando que se procurou "recolher informação detalhada sobre uma única unidade de estudo" (Santos & Lima, 2019, p. 36).

Para a recolha de dados, incidiu-se particularmente na utilização de instrumentos característicos da estratégia de investigação qualitativa, designadamente a análise documental e entrevistas semiestruturadas. A análise documental, baseada na recolha e análise de fontes documentais (Bryman, 2012, p. 543), foi utilizada ao longo de toda a investigação, contribuindo para a construção da base teórica e conceptual do estudo e na resposta ás QD 1, 2 e 3. As entrevistas semiestruturadas tiveram um papel fundamental na obtenção de dados que não havia sido possível obter a partir de fontes documentais (Freixo, 2012, p. 220), assumindo-se como instrumento essencial no desenvolvimento da investigação e na construção da resposta às QD 2 e 3.

Com a realização das entrevistas procedeu-se à observação dos dados obtidos através da análise de conteúdo, seguindo a tipologia temática ou categorial por permitir a interpretação do sentido do que foi dito, para além da descrição das situações (Santos & Lima, 2019, p. 119), tendo sido identificadas as unidades de contexto e determinadas as unidades de registo, tendo sido, consequentemente, quantificadas as unidades de registo traduzidas em percentagem. Dos dados obtidos foram evidenciados os resultados superiores a 50%, porque indicam que maioria dos participantes tem uma opinião ou posição semelhante em relação à questão, e enfatizados os resultados maiores ou iguais a 80%, por ser aqueles que indicam maior concordância entre os participantes. Em casos pontuais, dada a sua relevância para a investigação, foram ainda sublinhados resultados superiores a 25%.

Complementarmente, tendo em vista a coleta de dados mensuráveis, a amplitude da amostra e por forma a alcançar uma outra perspetiva do objeto de estudo, tornou-se igualmente relevante a utilização de instrumentos de recolha de dados característicos da estratégia de investigação quantitativa, em que se utilizou o inquérito por questionário do tipo fechado.

Neste âmbito, foi enfatizado o seu caráter objetivo (Santos & Lima, 2019, p. 27) na prossecução das respostas às QD 2 e 3. A análise das questões foi efetuada através da respetiva incidência percentual face à totalidade das respostas obtidas em cada grupo. Para os diferentes tipos de questões definiram-se diferentes

critérios de análise para a obtenção de dados congruentes, na medida em que para as questões fechadas dicotómicas, na sua totalidade de opção entre o sim e o não (Santos & Lima, 2019, p. 77) e para as questões de escolha múltipla em leque fechado, os resultados apresentaram-se percentualmente, sendo relevado o maior valor obtido no universo de respostas. A propósito das afirmações relativas à aferição do grau de concordância do seu conteúdo, utilizou-se a escala de Likert de cinco pontos (1- Nada relevante; 2- Pouco relevante; 3- Relevante; 4- Bastante relevante; 5- Muito relevante) (Likert, 1932, p. 47).

Seguidamente, os dados obtidos das respostas às QD 1, 2 e 3 foram analisados através de uma matriz SWOT, a fim de obter à resposta à QC. Pode-se observar um esquema que procura resumir o método utilizado na investigação.

Foram realizadas dez entrevistas, incidindo sobre uma amostra não-probabilística intencional (Santos & Lima, 2019) subdividida em três grupos. Conforme se pode observar no Quadro 1, o grupo A incluiu quatro elementos da equipa de desenvolvimento do projeto MOPREVIS da Universidade de Évora; o grupo B abrangeu quatro militares do CTer de Setúbal envolvidos no desenvolvimento e testagem da ferramenta; o grupo C abarcou dois altos responsáveis do comando da GNR com responsabilidade na condução a nível estratégico e operacional da instituição.

Tabela 1 – Lista de entrevistados

Entrevista	Entrevistado	Função	Data
A1	Professor Paulo Infante	Professor Associado da Universidade de Évora e membro da equipa de desenvolvimento do projeto MOPREVIS (Estatística)	27-03-2023
A2	Professor Vítor Nogueira	Professor Associado da Universidade de Évora e membro da equipa de desenvolvimento do projeto MOPREVIS (Informática)	28-03-2023
A3	Professor Pedro Nogueira	Professor Associado da Universidade de Évora e membro da equipa de desenvolvimento do projeto MOPREVIS (Sistemas de informação Geográfica).	27-03-2023
A4	Coronel (R) Paulo Jorge Silva Rebelo Manuel	Ex-Comandante do Comando Territorial de Setúbal da GNR e membro da equipa de desenvolvimento do projeto MOPREVIS	23-03-2023
B1	Tenente-Coronel Nuno Alexandre Carocha Gonçalves	2.º Comandante do Comando Territorial de Setúbal da GNR	22-03-2023
B2	Cabo-Chefe Paulo Jorge Dinis Rebisco	Investigador Criminal do Núcleo de Investigação de Acidentes de Viação do Destacamento de Trânsito de Setúbal da GNR	16-03-2023
B3	Capitão Hélder Alexandre de Sousa Lima	Atual Comandante do Destacamento de Trânsito de Setúbal da GNR	21-03-2023

[Cont.]

B4	Capitão Celso Leandro Fernandes Araújo Leones Pereira	Ex-Comandante do Destacamento de Trânsito de Setúbal da GNR	20-03-2023
C1	Tenente-General José Manuel Lopes dos Santos	Comandante-Geral da GNR	28-03-2023
C2	Coronel Luís Filipe Cristóvão Ferreira Branco	Comandante da Unidade Nacional de Trânsito da GNR	17-03-2023

As entrevistas realizadas tiveram por base um guião previamente edificado especificamente para cada um dos grupos de entrevistados. Todas as entrevistas foram efetuadas por correio eletrónico.

Em relação ao inquérito por questionário o mesmo compreendeu 24 questões, distribuídas por 3 secções. A secção I incide na caracterização geral dos participantes, a secção II sobre IA na prevenção e alerta da sinistralidade rodoviária e a secção III aborda o planeamento da atividade operacional dos Destacamentos de Trânsito da GNR.

Neste sentido, recorrendo-se à plataforma *google forms*, procedeu-se à elaboração de sete questões de escolha múltipla, nove questões dicotómicas e oito afirmações para atribuição do grau de concordância da população. Após a sua construção, realizou-se um pré-teste a elementos constituintes da população em análise.

Após validação, o inquérito por questionário foi aberto a 16 de março de 2023, tendo sido encerrado a 23 de março do mesmo ano. Foi divulgado e enviado o *link* do formulário através de correio eletrónico à população previamente definida (Hill & Hill, 2016, p. 41), constituída pelo universo total de Oficiais que desempenham funções de Comandante de Destacamento de Trânsito e de Adjunto do Comandante de Destacamento de Trânsito da GNR, num total de 35, de acordo com os dados fornecidos pelo Comando Operacional da GNR. Foram obtidas 33 respostas completas, totalizando 94% da população.

4. A INTELIGÊNCIA ARTIFICIAL NA PREVENÇÃO E ALERTA DA SINISTRALIDADE RODOVIÁRIA

4.1. A INTELIGÊNCIA ARTIFICIAL

As primeiras abordagens realizadas com algoritmos baseados em IA consistiam, principalmente, em projetos e investigações académicas, onde as suas aplicações se resumiam a provas de conceito, com pouco desenvolvimento no que poderiam ser futuras aplicações em larga escala. A evolução tecnológica recente, o aumento da comunidade científica a investigar esta temática e também o crescimento exponencial dos recursos alocados a este domínio, têm contribuído para que os algoritmos baseados em IA se tornem ferramentas essenciais e cada vez mais centrais, simplificando processos em tempos considerados complexos (Collins et al., 2021).

A utilização deste tipo de ferramentas nos diversos domínios, seja no mundo económico, financeiro, militar, saúde, transportes, entre outros, tem revelado que se trata de uma área em crescente desenvolvimento e que apresenta um sem número de potencialidades. Em 2020 a própria Comissão Europeia referiu "[…] ser essencial que as administrações públicas, os hospitais, os serviços de transporte e de utilidade geral pública, os supervisores financeiros e outros domínios de interesse público comecem rapidamente a utilizar produtos e serviços baseados na IA nas suas atividades" (Comissão Europeia, 2020, p. 9).

De facto, no mundo atual que se carateriza pelo rápido avanço tecnológico e pelos aumentos exponenciais dos grandes conjuntos de dados, a IA passou da mera teoria à aplicação real numa escala sem precedentes (Helm et al., 2020). Desde a análise de conjuntos de dados extraordinariamente grandes em tempo real, nos veículos autónomos, nas recomendações de visualização influenciadas pelo histórico, até recomendações de compra *on-line* e anúncios, a IA tornou-se fundamental em muitos setores da sociedade e muitas vezes funciona de forma invisível nos nossos dispositivos eletrónicos pessoais (Helm et al., 2020).

De entre as grandes potencialidades evidenciadas, destaca-se a "[…] utilização de sistemas baseados em IA nas organizações que tem melhorado a capacidade de tomada de decisão nos seus processos, bem como diminuído os custos associados às mesmas tomadas de decisão" (Raimundo & Sebastião, 2021, p. 5).

A IA tornou-se tão abrangente que existiu a necessidade de atribuir duas subáreas: o *Machine Learning* e o *Deep Learning*, conforme podemos analisar na Figura 2.

Figura 2 – A IA e as suas subáreas
Fonte: Raimundo e Sebastião (2021, p. 9).

4.2. A sinistralidade rodoviária

É consensual que a utilização dos veículos rodoviários constitui, na atualidade, um bem necessário e de manifesta utilidade social. A dinâmica da sociedade contemporânea apresenta como base de funcionamento a mobilidade, que procura ser cada vez mais rápida. Com efeito, parece que o Homem se tornou dependente da possibilidade de movimentação, que por sinal, se encontra baseada no uso intensivo de veículos rodoviários motorizados.

Ao longo da história, com o incremento da utilização dos veículos rodoviários, emergem os problemas associados às falhas e erros do sistema rodoviário, e que que culminam na ocorrência de sinistros rodoviários, provocando anualmente significativos custos humanos, económicos e sociais em todo o mundo.

Neste sentido, reconhecendo a relevância desta problemática, através da resolução n.º 74/299 da Assembleia Geral da ONU, os Estados assumiram o objetivo comum na década 2021-2030, de reduzir as vítimas mortais e feridos resultantes da sinistralidade rodoviária, em pelo menos 50%.

Para a consecução de tal objetivo a OMS estabeleceu um plano base numa abordagem que procura estabelecer a segurança rodoviária como um fator chave no desenvolvimento sustentável dos Estados. A segurança rodoviária deve ser encarada como um valor básico, um direito fundamental para qualquer ser humano, e só assim se "impulsionará a agenda global e criará um novo ímpeto para um compromisso maior de governos, corporações e organizações internacionais com vista à implementação de medidas que podem reduzir significativamente o trauma no trânsito" (OMS, 2021, p. 7).

O continente Europeu, no que respeita ao sistema rodoviário, apresenta níveis de segurança relativos elevados, tendo alcançado uma evolução bastante positiva nas últimas décadas. Observando o histórico da evolução da sinistralidade nos últimos anos, verifica-se uma tendência de descida até ao ano de 2013 após o qual estagnou sofrendo pequenas variações (European Commission, 2021). Portugal, em comparação com o resto dos países europeus, apresenta valores muito elevados, tendo registado, em 2020, 27.725 sinistros rodoviários com vítimas, dos quais resultaram 536 mortos. Estes valores colocam Portugal como o nono país da União Europeia com mais mortes por milhão de habitantes (Eurostat, 2021).

De acordo com Campón Domínguez (2019, p. 102), o sistema rodoviário é um sistema complexo e muito dinâmico, composto por uma série de elementos:

— O subsistema humano, composto pelos condutores dos veículos, peões e outros possíveis usuários das vias rodoviárias;

— O subsistema tecnológico representado, principalmente, pelo veículo a motor;

— O subsistema estrutural composto pela via, a sua envolvente e as circunstâncias em que se encontram ambos;

— E o subsistema normativo, composto pela legislação e pelos usos e costumes que disciplinam o comportamento dos anteriores três subsistemas.

Como tal, o exercício da condução implica, continuadamente, uma sequência dinâmica e heterogénea de ações interrelacionadas, o que conduz por vezes a resultados incertos e imprevisíveis (Leal, 2016). A instabilidade nos subsistemas que compõem o sistema rodoviário provoca um conflito nesse mesmo sistema, manifestando-se através de sinistros rodoviários. Para reduzir a sinistralidade rodoviária é necessário atuar em cada um desses subsistemas, garantindo o seu equilíbrio, e assim assegurar um elevado nível de segurança.

4.3. A INTELIGÊNCIA ARTIFICIAL E A SINISTRALIDADE RODOVIÁRIA

Nos estudos desenvolvidos na área da sinistralidade rodoviária, "[…] várias abordagens metodológicas têm sido utilizadas para analisar dados de sinistros rodoviários" (Infante, et al., 2022b). Perante uma visão geral das técnicas de análise de dados, vários algoritmos usados para construir predições de sinistros rodoviários e a identificação de vários fatores de risco são apresentados por Chand et al., (2021). Nas revisões da literatura apresentadas por Silva et al., (2020) e Gutierrez-Osorio

e Pedraza (2020), são apresentados vários modelos de *machine learning* para a predição de sinistros. Uma revisão sistemática sobre o estado da arte da predição de sinistros rodoviários em tempo real pode ser vista no trabalho de Hossain et al., - "*Realtime crash prediction models: State-of-the-art, design pathways and ubiquitous requirements*" (2019).

Com recurso à IA, e face aos atuais avanços dos métodos computacionais, os modelos baseados em algoritmos de *Machine Learning* (aprendizagem automática) têm-se revelado como ferramentas muito promissoras na investigação do fenómeno da sinistralidade rodoviária (Jamal et al., 2021, cit. por Infante et al., 2022a), especialmente no que respeita aos modelos preditivos.

Os modelos preditivos da sinistralidade rodoviária são um campo do conhecimento científico muito relevante e atual, aberto à inovação na pesquisa de algoritmos e técnicas de análise de dados que respondam ao desafio de criar um ambiente rodoviário cada vez mais seguro (Gutierrez-Osorio & Pedraza, 2020). Entre os métodos mais utilizados como modelos preditivos, conforme mostrado na Figura 3, podem considerar-se os seguintes: i) redes bayesianas; ii) computação evolutiva; iii) *support vector machines*; iv) redes neuronais artificiais; e v) aprendizagem profunda (Gutierrez-Osorio & Pedraza, 2020, p. 440).

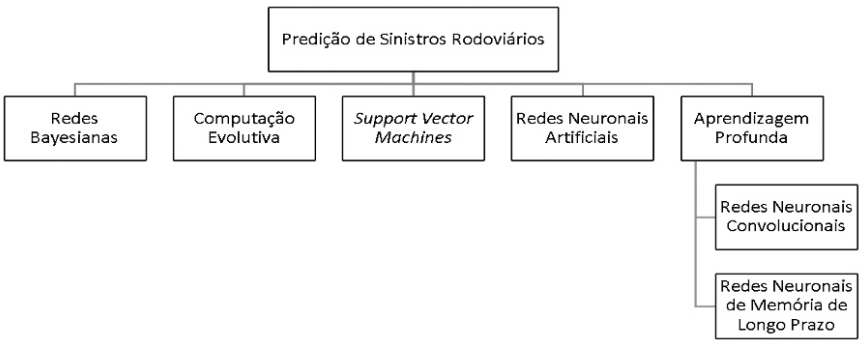

Figura 3 – Métodos e algoritmos representativos utilizados na predição de sinistros rodoviários
Fonte: Adaptado de Gutierrez-Osorio & Pedraza (2020, p. 441).

A predição de sinistros rodoviários é considerada um aspeto fulcral na segurança rodoviária, e será tanto melhor quanto mais informação usar das quatro dimensões associadas ao sinistro rodoviário: os dados dos veículos; os dados dos condutores; os dados das condições do tráfego rodoviário ou do seu histórico;

e os dados das condições meteorológicas. Qualquer combinação destas quatro perspetivas aumentará a precisão de um modelo preditivo (Halim et al., 2016).

Por outro lado, como se pode ver nas revisões bibliográficas já referidas (Chand et al., 2021; Silva et al., 2020; Gutierrez-Osorio & Pedraza, 2020; Hossain et al., 2019) os modelos preditivos são desenvolvidos em função do objetivo: gravidade do sinistro rodoviário ou das vítimas, frequência de sinistros ou ocorrência de sinistros.

A predição da gravidade do sinistro rodoviário geralmente explora a relação entre a sua gravidade ou vítimas e os fatores contribuintes (como comportamento do condutor, características do veículo, geometria e condições da estrada) fornecendo, aos meios de socorro e responsáveis pelo trânsito, informações importantes para implementar medidas com vista a reduzir os efeitos colaterais do sinistro rodoviário, como fornecer assistência médica mais rápida às pessoas feridas, reduzindo assim as vítimas.

Em Portugal não são conhecidos trabalhos publicados envolvendo modelos preditivos com técnicas de IA. Costa et al. (2018) desenvolveram um modelo estatístico que permite identificar os fatores que contribuem para a frequência de sinistros rodoviários envolvendo vítimas mortais e feridos em segmentos rodoviários (não cruzando áreas urbanas) de algumas estradas na região Norte[5].

Poder predizer a frequência de sinistros rodoviários num determinado segmento de estrada específico, permite melhorar o sistema de gestão de emergência, pois o tempo de reação será melhorado se houver um aviso prévio sobre quais os segmentos de estradas em que se prevê maior número de ocorrências num dado período de tempo, bem como alocar meios das forças de segurança de uma forma mais eficaz e oportuna, potenciando a sua atuação no âmbito da prevenção desses mesmos sinistros.

Todavia, os modelos preditivos de frequência apenas permitem agir por reatividade, enquanto os modelos preditivos de ocorrência em tempo real permitem agir por antecipação, ao possibilitar que sejam tomadas medidas para que o sinistro rodoviário possa ser evitado. E é aqui que o Projeto MOPREVIS pretende atuar. Os modelos de predição apresentados para a estrada nacional (EN) n.º 10, EN n.º 4, autoestrada A33 (incluí Ponte Vasco da Gama) e itinerário complementar n.º 1 nunca foram implementados em Portugal e a nível internacional não há conhecimento de aplicação de modelos preditivos para a ocorrência, em tempo

[5] EN n.º 14; EN n.º 101 e EN n.º 206.

real, de sinistros rodoviários, com a falta de informação em algumas variáveis de grande interesse, seja informações específicas sobre veículos que transitam na via ou a própria intensidade de tráfego.

5. O PROJETO MOPREVIS

5.1. Caraterísticas

Em 2018, o distrito de Setúbal registou dos mais elevados números de vítimas mortais a nível nacional (ANSR, 2018). Neste contexto, o CTer de Setúbal, que detém 94% das visas rodoviárias do distrito, ao deparar-se com este preocupante fenómeno, procurou o envolvimento científico da Universidade de Évora no sentido de ser estudado e investigado este problema (Infante et al., 2022a, p. 5).

De acordo com Infante et al. (2022a, p. 5), o CTer de Setúbal pretendia produzir segurança rodoviária na sua ZA através da aplicação de uma matriz científica, tendo por base os seguintes vetores:

- A explicação da Ciência para os factos que decorrem dos registos existentes para compreender a realidade;
- A construção de um instrumento preditivo da sinistralidade rodoviária para empenhamento racional dos recursos humanos e materiais da GNR;
- A integração de conhecimento e o empenhamento espaço temporal dos recursos da GNR, numa dimensão conhecida do meio policial como *Intelligence-Led Policing* (as operações policiais orientadas pelas informações, neste caso o conhecimento e a análise de risco);
- A redução do número de acidentes de viação e de vítimas e a otimização dos recursos.

Para tal, foi constituída uma equipa multidisciplinar composta por investigadores das áreas da Engenharia Informática, Estatística, Geociências, Ciências Sociais, Design e militares do CTer de Setúbal, nascendo assim o projeto MOPREVIS (Infante et al., 2022a, p. 6).

Com efeito, o MOPREVIS é um instrumento fundamentado e construído através de novas metodologias e tecnologias, designadamente a IA e a Ciência de dados (Infante et al., 2022a, p. 178), sobretudo no que respeita à análise explicativa dos sinistros rodoviários, tendo por base os dados dos registos oficiais do CTer de Setúbal, nomeadamente através do Boletim Estatístico do Acidente de Viação (BEAV) produzido por cada sinistro rodoviário registado pela GNR (Infante et al., 2022a, p. 8). Os dados utilizados consistem em 28.102 observações de sinistros

rodoviários de 2016 a 2019 contendo várias fontes de dados. Tendo por base esses dados, várias variáveis foram escolhidas e novas variáveis foram construídas (Santos et al., 2021, p. 5).

Na sua base final de análise o MOPREVIS é composto por 979 variáveis de diferentes tipos, designadamente: espaciais, temporais, ambientais, veículos envolvidos, intervenientes, via, tipologia e consequências do sinistro rodoviário, densidade populacional, intensidade de tráfego, etc., fornecidas pela Autoridade Nacional de Segurança Rodoviária (ANSR), o Instituto Português do Mar e da Atmosfera (IPMA), as Infraestruturas de Portugal (IP) e o *Waze* Portugal (Infante et al., 2022a, pp. 8-10).

Em relação à aplicação digital em si e ao seu funcionamento, esta permite a visualização do passado, presente e futuro, sendo possível selecionar o intervalo de tempo pretendido para a análise, visualização ou predição. Apresenta vários filtros, opções de análise e formas de apresentação de dados, como por exemplo representações gráficas, sendo oferecido ao utilizador a possibilidade de realizar um total de 218 representações gráficas (Infante et al., 2022a, p. 166). "Dispõe também de vários conteúdos informativos sobre os acidentes, nomeadamente relatórios, mapas e infografias desenvolvidas pela equipa MOPREVIS ao longo do projeto" (Infante et al., 2022a, p. 177).

Ao combinar um Sistema de Informação Geográfica (SIG) e modelos estatísticos, e aproveitando a capacidade do SIG para realizar análises espaciais complexas, esta ferramenta possibilitou identificar os principais fatores de sinistralidade rodoviária no CTer Setúbal (Infante, et al., 2022c, p. 2), tendo em conta que uma compreensão mais precisa dos fatores que influenciam o tipo de sinistro rodoviário, é fundamental para implementar estratégias apropriadas para melhorar a segurança (Infante, et al., 2023a, p. 2).

Contudo, a grande inovação desta ferramenta é a incorporação de uma parte preditiva que combina resultados da aplicação de metodologia estatística, análise espacial e modelos de IA. Com esta abordagem, é possível à ferramenta efetuar uma predição de *hotspots* de alto risco de ocorrência de sinistros rodoviários, bem como para determinados segmentos de via num determinado momento do dia (Infante, et al., 2023b, p. 2). Apesar de se encontrar ainda em fase experimental, este projeto já foi testado em ambiente real pelo CTer de Setúbal da GNR.

No que respeita aos dados recolhidos com as entrevistas, com a questão n.º 3 procurou- se apurar que resultados obteve o MOPREVIS nos testes em ambiente real (Quadro 2).

Pode-se observar que os resultados alcançados são bastante positivos, tendo em conta que 67% dos entrevistados referem que os dados obtidos nos testes da ferramenta em ambiente real são de elevada fiabilidade, tendo alcançado, em alguns casos, sensibilidades acima dos 80%. 67% dos entrevistados mencionam também que se trata de uma ferramenta que facilitou a tomada de decisão.

5.2. Potencialidades

Após o desenvolvimento do projeto científico, de acordo com Infante et al (2022a, pp. 6-7) o instrumento MOPREVIS apresenta as seguintes potencialidades:

- Definir os principais determinantes para a ocorrência dos vários tipos de acidente;
- Conceber um sistema de informação espacial sobre os acidentes (hotspots, e atlas de suscetibilidade de ocorrência de acidentes);
- Implementar um novo indicador de gravidade, mais robusto e consistente que os existentes;
- Traçar o perfil dos intervenientes num acidente de viação, condutores e vítimas;
- Analisar os acidentes de viação ocorridos em alguns concelhos de maior risco e contribuir para o apoio das entidades responsáveis pelo ordenamento do trânsito e intervenção nas respetivas vias;
- Avaliar as alterações provocadas pelo efeito da pandemia COVID-19 na sinistralidade rodoviária;
- Sensibilizar as principais instituições envolvidas na problemática da sinistralidade rodoviária, designadamente a GNR, a ANSR e as IP, para a necessidade de melhorar a qualidade dos dados e proceder à sua validação, bem como para a relevância e impacto dos mesmos na produção de políticas públicas de segurança rodoviária;
- Construir modelos preditivos para a ocorrência de acidentes em troços de 500 metros e de 2000 metros relativamente a quatro estradas do distrito de Setúbal, sinalizadas como de alto risco;
- Dotar a GNR de Setúbal com uma ferramenta digital de apoio à tomada de decisão, permitindo a otimização e a gestão dos recursos para a prevenção rodoviária, tratando-se de uma aplicação digital que permite a visualização do passado, presente e futuro.

Em relação aos dados obtidos nas entrevistas, com a questão n.º 1 pretendeu-

se aferir, de acordo com as respostas dos entrevistados, quais as principais potencialidades do MOPREVIS.

Perante os resultados obtidos, verifica-se que as principais potencialidades do MOPREVIS provêm do facto de, por um lado, a ferramenta permitir a otimização de recursos, com 50% dos entrevistados a incidir neste aspeto e por outro, de se constituir como um apoio na tomada de decisão, com 75% dos entrevistados a referir este facto. Destaca-se ainda que 38% dos entrevistados aponta a potencial redução da sinistralidade, a identificação dos fatores que potenciam a ocorrência de sinistros rodoviários e o modelo preditivo para as vias de elevado risco de sinistralidade, como potencialidades de relevo.

5.3. Limitações

Através da análise documental foi possível detetar algumas das limitações e constrangimentos mais relevantes, que afetaram, atrasaram ou inviabilizaram as investigações deste projeto, designadamente as seguintes:

- A fraca qualidade dos dados oficiais, que levou a que a base dos acidentes apenas ficasse estável em meados de 2019 devido a uma disponibilização tardia dos dados pretendidos e a um deficiente preenchimento do BEAV (…);
- Atraso muito grande na atualização/disponibilização de dados por parte da ANSR e dos dados meteorológicos por parte do IPMA;
- Dificuldade em estimar variáveis importantes, como a intensidade de tráfego, a velocidade dos veículos, taxa de álcool dos condutores, idade do parque automóvel, diversas características dos condutores e mesmo os dados meteorológicos que deveriam ser fornecidos em tempo real e facilmente incorporados na ferramenta digital;
- A pandemia COVID-19, que alterou o comportamento dos condutores e a mobilidade em geral;
- A disponibilização muito tardia dos dados relativos às sentenças dos processos-crime que envolveram acidentes com vítimas mortais e a não disponibilização de todos os relatórios de investigação que envolvem vítimas mortais (…)". (Infante et al., 2022a, p. 165)

Através da Questão n.º 2 das entrevistas, procurou-se apurar quais as principais limitações do MOPREVIS identificadas pelos entrevistados (Quadro 4).

A este propósito podemos observar que 75% dos entrevistados considera que a principal limitação do MOPREVIS é a sua dependência da qualidade dos

dados. Para além desta limitação, a não existência/disponibilização de outras variáveis de análise para além das já incorporadas e a dificuldade de comunicação entre as instituições ou entidades participantes, são também referidas como limitações por 38% dos entrevistados, indo ao encontro das condicionantes e limitações apontadas na revisão da literatura.

6. A APLICAÇÃO DO PROJETO MOPREVIS NA ZONA DE AÇÃO DA GUARDA NACIONAL REPUBLICANA

6.1. A promoção da segurança rodoviária pela Guarda Nacional Republicana

Nos termos da alínea f) do n.º 1 do artigo 3.º da Lei n.º 63/2007, de 06 de novembro, uma das atribuições da GNR consiste em "Velar pelo cumprimento das leis e regulamentos relativos à viação terrestre e aos transportes rodoviários, e promover e garantir a segurança rodoviária, designadamente, através da fiscalização, do ordenamento e da disciplina do trânsito". O Regulamento Geral de Serviço da GNR, no seu artigo 179.º, acrescenta ainda que:

> (…)
> 2 — Compete ainda garantir a fiscalização, o ordenamento e a disciplina do trânsito em todas as infraestruturas constitutivas dos eixos da Rede Nacional Fundamental e da Rede Nacional Complementar, dentro da sua área de responsabilidade.
> 3 — O efetivo da Guarda presta, por iniciativa própria ou a pedido, auxílio aos utentes das vias públicas, promovendo com urgência o socorro dos doentes e sinistrados pelo modo mais adequado. (Despacho n.º 10393/2010, de 05 de maio, 2010)

No que diz respeito ao planeamento estratégico da GNR, o domínio da segurança rodoviária também mereceu especial atenção, pelo que a Estratégia da Guarda 2025 vem estabelecer como objetivo estratégico n.º 15 o seguinte:

> Dinamizar a vigilância da rede viária fundamental e complementar, valorizando a aposta na prevenção, presença, visibilidade, consciencialização e fiscalização seletivas, direcionadas para os comportamentos, atitudes, grupos, áreas e períodos potencialmente causadores de insegurança e sinistralidade rodoviárias, através da coordenação centralizada, integrada e coordenada com as demais valências da Guarda. (Guedelha, 2020, p. 80)

Com efeito, no âmbito rodoviário, a GNR detém à sua responsabilidade a quase totalidade da rede viária nacional, apresentando cerca de 98% do território (Guedelha, 2020, p. 26), pelo que se acentua a importância do seu papel neste domínio. Neste sentido a GNR desempenha um papel primordial no sistema rodoviário português, sendo uma das entidades com elevado comprometimento na promoção da segurança rodoviária em Portugal e cuja atuação pode, de facto, ter um efeito verdadeiramente diferenciador.

Efetivamente, as ações de patrulhamento rodoviário e de fiscalização, direcionadas para a observação e controlo da conduta do fator humano, no âmbito da segurança rodoviária, são um dos mecanismos mais eficazes de persuasão e de mudança de comportamentos dos condutores (Zaal, 1994). Neste sentido, uma fiscalização e patrulhamento rodoviário eficaz e eficiente, mobilizado de acordo com critérios de prevenção bem definidos com o auxílio da ciência, poderá permitir uma diminuição sustentada e consistente da sinistralidade rodoviária e das suas consequências, podendo a IA, neste âmbito, desempenhar um papel de extrema relevância. E de facto, este parece ser o entendimento dos Comandantes de Destacamento de Trânsito da GNR.

Através da Secção II do inquérito por questionário, procurou-se perceber qual a perceção dos Comandantes de Destacamento de Trânsito sobre a importância da ciência, da IA e das suas ferramentas, na prevenção e alerta da sinistralidade rodoviária, através das Questões n.º 6 (Figura 4), n.º 7 (Figura 5) e n.º 8 (Figura 6).

Como observável nos resultados obtidos, a grande maioria dos inquiridos considera bastante ou muito relevante a ciência para o estudo e análise dos sinistros rodoviários, a importância das ferramentas baseadas em IA no combate à sinistralidade rodoviária, e a utilização de um instrumento preditivo no âmbito da sinistralidade rodoviária por parte da GNR.

A este propósito, parece resultar evidente que a grande maioria dos inquiridos reconhece a importância da ciência, da IA e das suas ferramentas, no estudo, na pesquisa e na melhoria da eficácia e da eficiência dos recursos no combate ao fenómeno da sinistralidade rodoviária, não oferecendo qualquer resistência à evolução de novas formas de abordagem a esta problemática.

6.2. O planeamento da atividade operacional da Guarda Nacional Republicana no âmbito da segurança rodoviária

O planeamento da atividade operacional da GNR, no âmbito da segurança rodoviária, envolve duas grandes áreas. A área preventiva, orientada para um fim futuro e que consiste em impedir que um perigo surja ou se concretize em dano e que se apresenta como a principal função de uma força de segurança (Sousa, 2003, p. 49), sendo alcançável essencialmente recorrendo ao patrulhamento rodoviário (GNR, 1997, pp. I-1). E a área repressiva, ou de prevenção indireta, que consiste numa reação a um ilícito, conhecido ou suspeito (Sousa, 2003, p. 49), que se apresenta como indispensável para a eficácia da prevenção e que se materializa em ações de fiscalização (GNR, 1997, pp. I-1; I-7).

Deste modo, ao longo do ano são planeadas campanhas de fiscalização e de intensificação de patrulhamento a nível nacional, que são projetadas em consonância com as políticas europeias e nacionais de segurança rodoviária, bem como com os períodos em que tradicionalmente se verifica um aumento significativo do tráfego rodoviário. O planeamento destas campanhas, quando realizado ao nível do Comando Operacional da GNR, materializa- se em Diretivas Operacionais[6], que são difundidas às Unidades para planeamento nas respetivas ZA, dando lugar a Ordens de Operações e à execução de operações dirigidas a fatores, grupos e locais específicos.

Paralelamente, as Unidades e respetivos Destacamentos de Trânsito elaboram o seu próprio planeamento no âmbito da fiscalização e patrulhamento que executam na atividade diária, procurando orientar o esforço para potenciar a redução de comportamentos de risco e contribuir assim para a redução da sinistralidade rodoviária na respetiva ZA.

Neste contexto, para além das orientações estratégicas, políticas ou internacionais, importa para a presente investigação analisar quais os elementos ou fatores em que a GNR se fundamenta para orientar o planeamento da fiscalização e do patrulhamento rodoviário, observando se os mesmos apresentam concordância com os principais elementos de informação fornecidos pelo MOPREVIS, designadamente, as principais determinantes da sinistralidade rodoviária, a informação espacial, o perfil dos intervenientes e os dados preditivos.

Por conseguinte, a Secção III do inquérito por questionário foi especialmente direcionada para identificar se essa tipologia de dados é tida em consideração no

[6] Em 2023 temos o exemplo da Diretiva Operacional n.º 04/23 – Campanha "PNF 2023", Diretiva Operacional n.º 11/23 – Campanha "ECR 2023", ou a Diretiva Operacional n.º 12/23 – Campanha "ROADPOL", entre outras.

planeamento da atividade operacional, se alguma das ferramentas de Comando e Controlo (C2) existente permite obter essa informação, bem como apurar a relevância da existência de uma ferramenta que permita obter esses dados, caso sejam tidos em falta.

Primeiramente pretendeu-se identificar quais os principais elementos em que os inquiridos se baseiam para o planeamento da fiscalização e do patrulhamento rodoviário. Apesar da quase totalidade dos inquiridos se fundamentar na análise estatística da sinistralidade, sublinha-se o facto da existência de elevadas percentagens de inquiridos que levam também em consideração fatores como a perceção ou conhecimento empírico, o volume de tráfego, ou a análise estatística das zonas onde ocorre a prática reiterada de infrações rodoviárias, o que poderá ser revelador da falta de critérios de cientificidade na abordagem à sinistralidade rodoviária, conduzindo a uma atividade operacional pouco eficaz e eficiente.

Relativamente à pertinência da informação relativa às principais determinantes da sinistralidade rodoviária, com efeito, podemos observar que uma elevada percentagem de inquiridos, 75,8 %, toma em consideração as principais determinantes da sinistralidade rodoviária no planeamento da atividade operacional, apesar de apenas 54,5% referir que dispõe atualmente de ferramentas que fornecem essa informação. Todavia, verifica-se que a quase totalidade considera como muito relevante (90,9%) a existência de uma ferramenta que forneça esses dados.

No respeitante à informação espacial da sinistralidade e à perceção dos inquiridos sobre a necessidade de melhoramento do atual indicador de gravidade em uso por parte da ANSR. Constata-se que praticamente todos os inquiridos, 97%, têm em consideração a informação espacial relativa à sinistralidade rodoviária no planeamento, verificando-se que a grande maioria (78,8%) dispõe de ferramentas de C2 que lhe permite obter essa informação. Quanto à sua relevância, resulta evidente que se trata de informação de extrema utilidade, tendo em conta que a totalidade dos inquiridos se refere a estes dados como muito relevantes (90,9%) e bastante relevantes (9,1%). No que diz respeito ao indicador de gravidade em uso por parte da ANSR, observa-se que a grande maioria dos entrevistados (75,8%) considera a necessidade do seu melhoramento.

Relativamente à informação relativa ao perfil dos intervenientes em sinistros rodoviários, extrai-se da análise que grande parte dos inquiridos (66,7%) não tem em consideração no planeamento o perfil dos intervenientes na sinistralidade rodoviária, pese embora tal facto possa resultar da não disponibilidade de uma

ferramenta de C2 que forneça essa informação, tendo em conta que 57,6% dos inquiridos refere não dispor dessa ferramenta, e a sua grande maioria considera que a sua existência seria muito relevante (54,5%) e bastante relevante (24,2%).

Dos resultados apresentados, a propósito da informação preditiva, releva-se o facto de a quase totalidade dos inquiridos referir não dispor de qualquer ferramenta de C2 e de considerar a sua existência como bastante relevante e muito relevante.

A este propósito, atendendo ao facto do MOPREVIS se materializar numa aplicação digital que disponibiliza dados do passado, do presente e do futuro, procurou-se apurar qual a relevância de uma aplicação com estas caraterísticas para o apoio à tomada de decisão, no âmbito do planeamento operacional da GNR. Da observação dos resultados surge claro que se trata de algo muito relevante para a quase totalidade dos inquiridos.

6.3. Requisitos para implementação do projeto MOPREVIS na zona de ação da Guarda Nacional Republicana

Considerando um eventual alargamento do MOPREVIS a toda a ZA da GNR, torna- se pertinente estudar quais as implicações que esta medida acarreta. Neste contexto, a investigação procurou analisar os seguintes aspetos: as alterações que serão necessárias efetuar no MOPREVIS; as condições necessárias, por parte da GNR, para a implementação e funcionamento do instrumento; quais os impactos que podem advir para a atividade operacional; se existem condições para um eventual projeto com a Fundação para a Ciência e Tecnologia (FCT); e, fundamentalmente, se a GNR considera relevante, viável e oportuno a eventual implementação desta aplicação digital no combate à sinistralidade rodoviária.

Assim, procurou-se identificar quais as alterações necessárias efetuar no MOPREVIS para a sua implementação em toda a ZA. Nesta senda, a totalidade dos entrevistados (100%) refere ser necessário desenvolver meios para a medição de variáveis importantes e paras as quais não existe informação; a grande maioria (75%) menciona a necessidade de automatização e melhoria do processo de fluxo e validação de dados; e metade (50%) refere ainda a necessidade de criar ou adaptar as abordagens usadas no âmbito dos fatores determinantes da ocorrência de sinistros rodoviários.

De forma a apurar quais as condições necessárias, por parte da GNR, para a implementação e funcionamento, eficaz e eficiente, do MOPREVIS em toda a ZA. No que respeita à fase de implementação, a grande maioria dos entrevistados assinala a necessidade de efetuar uma validação rigorosa dos dados históricos relativos à sinistralidade rodoviária em toda a ZA da GNR (75%); a criação de um processo que garanta rigor na recolha dos dados (75%); e a criação de um fluxo de dados referente à sinistralidade rodoviária em tempo real (63%). Uma pequena percentagem dos entrevistados alude ainda à criação uma rede de colaboração com outras entidades no fornecimento de dados complementares aos recolhidos pela GNR (atmosféricos, velocidades, tráfego, mortos a 30 dias etc.) como por exemplo a ANSR (25%) bem como a criação de canais de comunicação entre a GNR e as equipas de desenvolvimento (25%).

Quanto à fase de utilização, garantir o rigor na recolha dos dados dos sinistros rodoviários, como por exemplo alterar o BEAV, surge novamente para a maioria dos entrevistados como a condição a garantir para o funcionamento eficaz e eficiente do MOPREVIS. Com menor incidência, releva-se ainda a atualização dos dados da sinistralidade rodoviária (quase) em tempo real (38%); manter canais de comunicação entre a GNR e as equipas de desenvolvimento (25%); e o apoio à aplicação da ferramenta no terreno, a capacitação dos seus operacionais e a sua monitorização (25%).

De forma a perceber qual o tempo estimado necessário para a implementação e funcionamento, em pleno, do MOPREVIS em toda a ZA. Apurou-se que não se afigura possível determinar qual o tempo estimado, tendo em conta a dispersão de resultados obtidos que variam de 1 a 5 anos.

De forma a avaliar que implicações poderá acarretar para a atividade operacional, procurou-se apurar quais os impactos positivos e negativos. Podemos observar que a totalidade (100%) dos entrevistados é da opinião que a introdução do MOPREVIS no planeamento da atividade operacional teria um impacto positivo. Destes, 83% considera que o impacto positivo seria no aumento da eficiência da atividade desenvolvida; 67% no facto de ser uma ferramenta de apoio à decisão, e 33% considera que seria uma evolução da abordagem na prevenção de sinistros rodoviários. Quando questionados sobre eventuais impactos negativos, 67% dos entrevistados considera não se verificar qualquer impacto negativo na implementação do MOPREVIS. Contudo, a possível afetação de recursos humanos, os potenciais desvios nos parâmetros da predição e a probabilidade de existir o

condicionamento da decisão no que respeita à gestão de recursos, é apontado por 17% dos entrevistados como um eventual impacto negativo.

Procurou-se determinar se os inquiridos consideram existir condições para um possível projeto em colaboração com FCT e Universidade de Évora, para o estudo e implementação do MOPREVIS em toda a ZA da GNR. Verifica-se que metade dos entrevistados (50%) observam condições favoráveis à existência de um eventual projeto em colaboração coma FCT. Todavia, a outra metade (50%) refere que tal facto se encontra dependente da FCT.

De forma a averiguar se a GNR considera relevante, viável e oportuno a eventual implementação desta aplicação digital no combate à sinistralidade rodoviária, resulta evidente que os entrevistados consideram extremamente relevante a implementação de uma ferramenta como o MOPREVIS no combate à sinistralidade rodoviária, permitindo desenvolver um planeamento mais eficiente das ações de patrulhamento e fiscalização rodoviária. Verifica-se, ainda, que os entrevistados consideram viável e oportuna a disseminação do projeto a outros distritos. Como tal, constata-se a existência de disponibilidade por parte do Comando da Guarda para uma eventual implementação do MOPREVIS em toda a sua ZA. Além do mais, parece já existir algum conhecimento sobre a ferramenta digital no seio da GNR. Pretendeu-se aferir o conhecimento dos inquiridos sobre a existência do projeto MOPREVIS e qual a forma como obtiveram esse conhecimento, verificou-se que cerca de metade (51,5%) tinha conhecimento sobre a sua existência. Destes, grande parte obteve essa informação através de outros militares da GNR (50%).

7. ANÁLISE SWOT

Na prossecução da resposta à QC desta investigação, e de acordo com o percurso metodológico inicialmente preconizado, seguidamente elabora-se uma análise SWOT centrada nos dados anteriormente recolhidos.

A análise SWOT é uma ferramenta frequentemente utilizada no planeamento estratégico, que visa identificar as potencialidades e as vulnerabilidades de uma organização ou projeto, bem como as oportunidades e ameaças reveladas na análise do ambiente externo (Carapeto & Fonseca, 2014, p. 169). Com esta análise, pretende-se identificar as áreas onde poderá ser necessário adotar medidas corretivas ou de melhoria, bem como as oportunidades que podem ser exploradas.

Neste sentido, pretende-se efetuar uma análise SWOT à aplicação de uma ferramenta de IA na prevenção e alerta da sinistralidade rodoviária, utilizando como caso de estudo o projeto MOPREVIS e a sua implementação na ZA do CTer de Setúbal, sustentada nos dados obtidos nas respostas às QD 1, 2 e 3. Seguindo esta trajetória, da análise resultaram os seguintes dados (Quadro 14).

Tabela 2 – Análise SWOT

Fatores Endógenos		Fatores Exógenos	
Potencialidades	**Vulnerabilidades**	**Oportunidades**	**Ameaças**
- Melhoria da capacidade de tomada de decisão nos processos das organizações; - Ferramenta promissora no estudo e investigação do fenómeno da sinistralidade rodoviária; - Melhoraria do sistema de gestão de emergência; - Permite alocar meios das forças de segurança de uma forma mais eficaz e oportuna; - Os seus modelos preditivos permitem agir por antecipação; - Permite obter informação do passado, presente e futuro; - Elevada fiabilidade dos resultados alcançados nos testes reais;	- Forte dependência da qualidade dos dados; - Dificuldade em estimar outras variáveis de análise para além das já incorporadas; - Processo de fluxo de dados não automatizado; - Necessidade de adaptar as abordagens usadas para cada Zona de Ação;	- GNR como elemento crucial no combate à sinistralidade rodoviária; - Planeamento da atividade operacional da GNR sustentado na IA; - Falta de informação nas atuais ferramentas de C2 da GNR; - Criação de um fluxo de dados em tempo real pela GNR; - Criação de um processo que garanta rigor na recolha dos dados pela GNR; - Disponibilidade por parte da GNR para uma eventual implementação de ferramenta baseada em IA em toda a sua Zona de Ação;	- Atraso na disponibilização de dados por parte de outras entidades; - Dificuldade de comunicação entre instituições ou entidades participantes; - A não disponibilização de dados por parte de outras entidades;

Desta matriz, resultam as ideias-chave que permitem desenvolver as Linhas de Orientação Estratégica (LOE) que enformam o processo, através do qual, poderão ser potenciados os contributos da IA na prevenção e alerta da sinistralidade rodoviária, dando resposta à QC da presente investigação. Por conseguinte, é possível materializar as quatro LOE seguintes.

LOE1 – Assegurar qualidade e rigor. Como observado, a qualidade dos dados é uma vulnerabilidade importante na aplicação da IA à prevenção da sinistralidade rodoviária. Garantindo a precisão e a integridade dos dados, é possível aumentar a eficácia da análise e predição. De forma a mitigar o risco de utilização de dados de fraca qualidade, é necessário implementar mecanismos de verificação e validação.

Relativamente ao estudo de caso, torna-se assim importante que a GNR crie um processo de validação dos seus dados históricos e aperfeiçoe os procedimentos de recolha de dados dos futuros sinistros rodoviários, garantindo deste modo o rigor dos elementos obtidos, que, por conseguinte, permitirá obter maior eficácia da ferramenta MOPREVIS.

LOE2 – Automatizar. A automatização do fluxo de dados reduz a possibilidade de ocorrência de erros humanos, aumentando a precisão e a confiabilidade dos dados. Além disso, a automatização permite uma maior agilidade na obtenção e processamento dos dados, possibilitando a tomada de decisão mais rápida e eficiente. Para criar um processo automático de fluxo de dados, é necessário implementar soluções que permitam a transferência automática de dados em tempo real.

Outra vantagem que a automatização pode permitir é a integração de diferentes fontes de dados, possibilitando uma visão mais abrangente e completa da sinistralidade rodoviária. Com efeito, a automatização do fluxo de dados que alimentam o MOPREVIS, pode ser uma medida importante para aprimorar a sua eficiência, possibilitando uma análise mais precisa e uma tomada de decisão mais ágil e eficiente.

LOE3 – Desenvolver e diversificar. Para melhorar a capacidade preditiva das ferramentas de IA, é importante desenvolver e incorporar variáveis adicionais, de forma a obter uma análise mais abrangente e precisa. Quanto mais variáveis relevantes forem incorporadas, mais a análise pode ser refinada e ajustada para obter resultados mais rigorosos.

Em relação ao estudo de caso, a título de exemplo, pode ser equacionado a inclusão de dados de câmaras de vigilância das concessionárias, sensores de tráfego, medidores de velocidade, entre outros, de forma a monitorizar a rede viária e detetar potenciais situações de risco ou de perigo.

LOE4 – Cooperar e colaborar. Estabelecer protocolos de colaboração entre as várias entidades envolvidas no combate à sinistralidade rodoviária, sejam entidades governamentais, não governamentais ou empresas privadas, é algo essencial para fomentar a cooperação e partilha de informações e dados. Além disso, das boas relações institucionais, resulta a criação de canais de comunicação técnicos diretos, fundamentais para ultrapassar determinados constrangimentos, identificar e abordar áreas problemáticas e tomar medidas preventivas para, no caso em apreço, reduzir a sinistralidade rodoviária. Por outro lado, a colaboração

pode também levar ao desenvolvimento de soluções tecnológicas inovadoras e de sinergias.

Neste contexto, no atinente ao MOPREVIS, será relevante desenvolver protocolos que definam claramente as diretrizes relativas à partilha de informações e dados, mas, em especial, que fomentem a colaboração entre as instituições.

8. CONCLUSÕES

O preocupante fenómeno da sinistralidade rodoviária enforma já longos anos. Os primeiros automóveis a circular em Portugal surgem no século XIX. À medida que vai crescendo o número de veículos automóveis em circulação, as autoridades nacionais tomam consciência da importância que o automobilismo apresenta para o desenvolvimento do país, percebendo igualmente que a utilização deste tipo de veículos trazia novos problemas de segurança, designadamente pela gravidade dos sinistros rodoviários que podiam originar.

Na atualidade, a segurança rodoviária é dos temas que mais preocupam a comunidade mundial. Para além dos impactos económicos e sociais que lhe estão associados, revela-se um grave problema de saúde pública, face aos milhões de vítimas que, por ano, morrem ou ficam com sequelas graves decorrentes de sinistros rodoviários, com a agravante de constituir a principal causa de morte de crianças e jovens adultos.

No entanto, os perigos subjacentes à sinistralidade rodoviária podem ser prevenidos, ou pelo menos mitigados. O recurso a sistemas baseados em IA, na área da segurança rodoviária, já constitui uma realidade, apresentando resultados bastante relevantes, em especial, no que respeita aos modelos preditivos. Com custos relativamente reduzidos, estas ferramentas podem oferecer uma base científica e sólida no apoio à avaliação e seleção de medidas de segurança rodoviária, bem como no apoio ao processo de tomada de decisão das organizações.

Em Portugal, já foram dados os primeiros passos neste domínio, principalmente através de projetos de investigação desenvolvidos por algumas Academias. A este propósito, destaca-se o projeto da Universidade de Évora, desenvolvido em parceria com o CTer de Setúbal, o MOPREVIS. O objetivo principal deste projeto, passa pela redução da sinistralidade grave no distrito de Setúbal através da construção de uma ferramenta digital que apoie, em tempo real, a tomada de decisão e o planeamento da atividade operacional. Ainda em fase experimental, e limitado à ZA do CTer de Setúbal, este projeto exibe um modelo

bastante evoluído e consolidado, que aparenta possuir um elevado potencial de intervenção no combate à sinistralidade rodoviária.

Neste contexto, partindo do argumento que a aplicação de metodologias de IA na construção de modelos preditivos potencia a prevenção e o alerta da sinistralidade rodoviária, afigurou-se assim pertinente, analisar de que forma podem ser potenciados esses contributos da IA no combate ao flagelo da sinistralidade rodoviária.

Perante este enquadramento, procedeu-se à edificação de um modelo de análise, que permitisse analisar a problemática em estudo, e que culminasse na apresentação de soluções materializadas em linhas de orientação estratégica, no sentido de alcançar o OG previamente definido. Com efeito, para a prossecução desse desiderato, foi estabelecida a QC no sentido de se analisar de que forma podem ser potenciados os contributos da IA para a prevenção e alerta da sinistralidade rodoviária, usando como caso de estudo o modelo MOPREVIS, na perspetiva de uma eventual aplicação desta ferramenta em toda a área de atuação da GNR.

Destarte, para o presente estudo recorreu-se a uma metodologia de raciocínio indutivo, através de uma estratégia mista, que permitiu obter resposta às três QD identificadas. A recolha de dados resultou da correlação de técnicas de análise documental e inquéritos por entrevista, reforçada com dados obtidos através de inquéritos por questionário, culminando na elaboração de uma matriz SWOT.

Seguindo esta trajetória, e em resposta à QD1, "Quais os principais contributos teóricos da IA para a prevenção e o alerta da sinistralidade rodoviária?", conclui-se que as ferramentas de IA, neste âmbito, se podem constituir como um importante apoio no processo de tomada de decisão das organizações, além de permitirem melhorar o sistema de gestão de emergência e de potenciarem a atuação preventiva das forças de segurança.

A mobilidade é efetivamente um dos pilares fundamentais da sociedade contemporânea, que procura ser cada vez mais ágil, pelo que a utilização de veículos rodoviários constitui um bem necessário e de manifesta utilidade social. Com o incremento do uso de veículos rodoviários, surgem problemas associados a falhas e erros do sistema rodoviário, os quais culminam em sinistros rodoviários, gerando anualmente significativos custos humanos, económicos e sociais. Portugal apresenta índices preocupantes de sinistralidade rodoviária, figurando entre

os nove países da União Europeia com maior número de mortes por milhão de habitantes.

As ferramentas baseadas em IA são uma área bastante promissora e em acentuada evolução, que apresenta inúmeras potencialidades, nas quais tem especial relevo a melhoria da capacidade de tomada de decisão nos processos organizacionais. Além disso, os modelos preditivos baseados em algoritmos de Machine Learning possibilitam predizer a frequência de sinistros rodoviários num determinado segmento de via específico, o que poderá contribui para melhorar o sistema de gestão de emergência, pois o tempo de reação será melhorado se houver um aviso prévio sobre quais os segmentos de vias em que se prevê maior número de ocorrências num dado período, bem como alocar meios das forças de segurança de uma forma mais eficaz e oportuna, potenciando a sua atuação no âmbito da prevenção.

Não obstante esta importante contribuição, os modelos preditivos de frequência possibilitam apenas uma atuação reativa, enquanto os modelos preditivos de ocorrência em tempo real permitem uma atuação proativa, permitindo a adoção de medidas capazes de evitar o sinistro rodoviário. É neste contexto que o projeto MOPREVIS poderá oferecer o seu maior contributo.

Seguidamente, partiu-se para a resposta à QD2: "quais as principais caraterísticas, potencialidades e limitações do projeto MOPREVIS?", relevando neste âmbito que se trata de um instrumento desenvolvido com base em metodologias e tecnologias inovadoras, incluindo IA e Ciência de Dados. A base de análise é composta por 979 variáveis de diversos tipos, tais como espaciais, temporais, ambientais, veículos envolvidos, intervenientes, via, tipologia e consequências do sinistro rodoviário, densidade populacional, intensidade de tráfego, entre outras, fornecidas por diversas entidades.

No que respeita ao funcionamento da aplicação digital, é possível obter informações do passado, presente e futuro, e selecionar o intervalo de tempo desejado para análise, visualização ou predição.

Sobre as principais potencialidades destaca-se o facto de permitir conceber um sistema de informação espacial sobre a sinistralidade rodoviária; implementar um novo indicador de gravidade; traçar o perfil dos intervenientes num sinistro rodoviário; construir modelos preditivos para a ocorrência de sinistros rodoviários; apoio à tomada de decisão; e otimização e gestão dos recursos.

Respeitante às principais limitações identifica-se a sua dependência da qualidade dos dados; o atraso na atualização ou não disponibilização de dados por parte de outras entidades; a dificuldade em estimar outras variáveis de análise; e a dificuldade de comunicação entre as instituições ou entidades participantes.

Nesta senda, prosseguiu-se para a resposta à QD3, "Quais as condições para aplicação do MOPREVIS a toda a ZA da GNR?", observando-se que, para tal suceder, existe a necessidade de efetuar determinadas modificações no MOPREVIS, bem como desenvolver e adaptar alguns processos por parte da GNR, principalmente no que respeita à recolha e tratamento de dados.

O facto de a GNR ter a quase totalidade da rede viária nacional sob sua responsabilidade confere um peso primordial ao seu papel neste domínio, permitindo-lhe atuar como elemento diferenciador no sistema rodoviário português. Para além das orientações estratégicas, políticas ou internacionais, os Comandantes de Destacamento de Trânsito fundamentam grande parte do seu planeamento da atividade operacional diária na análise estatística da sinistralidade. Com menor incidência, verifica-se que também ponderam fatores como a perceção ou o conhecimento empírico, o volume de tráfego ou a análise estatística das áreas onde se praticam reiteradamente infrações rodoviárias. Esta abordagem poderá ser indicativa de alguma falta de dados e de critérios de cientificidade, podendo o MOPREVIS, neste âmbito, desempenhar um papel de extrema relevância, já que se constata por parte da GNR a existência de disponibilidade para uma eventual implementação do MOPREVIS em toda a sua ZA.

Assim, no que concerne às alterações necessárias efetuar ao MOPREVIS salienta-se a necessidade de desenvolver meios para a medição de variáveis importantes e paras as quais não existe informação; automatizar e melhorar o processo de fluxo de dados e a sua validação; e criar ou adaptar as abordagens usadas no âmbito dos fatores determinantes da ocorrência de sinistros rodoviários.

Por seu turno, por parte da GNR, é essencial efetuar uma validação rigorosa dos dados históricos relativos à sinistralidade rodoviária em toda a sua ZA; criar um processo que garanta rigor na recolha dos dados das futuras ocorrências; criar um fluxo de dados referente à sinistralidade rodoviária em tempo real; e garantir o rigor na recolha dos dados dos sinistros rodoviários.

Destarte, em linha com o OG proposto, apresentou-se a resposta subjacente à QC, enformada por quatro LOE resultantes das ideias-chave obtidas na elaboração da matriz SWOT. Neste particular, conclui-se que a forma de potenciar os contributos da IA para a prevenção e alerta da sinistralidade rodoviária deve ser sustentada nas seguintes LOE:

LOE1 – Assegurar qualidade e rigor. A qualidade dos dados constitui uma das maiores vulnerabilidades das ferramentas baseadas em IA. Á luz do referido, garantindo a precisão e a integridade dos dados, ao implementar mecanismos de verificação e validação, é possível aumentar a eficácia da ferramenta na análise e predição;

LOE2 – Automatizar. A automatização do fluxo de dados apresenta-se como uma solução capaz de minimizar a probabilidade de ocorrência de erros provenientes de intervenções humanas, fato que, por sua vez, contribui para o aumento da precisão e da confiabilidade dos dados. Além disso, permite a obtenção e o processamento dos dados de forma mais célere e eficiente, propiciando, assim, uma tomada de decisão mais ágil;

LOE3 – Desenvolver e diversificar. A fim de aprimorar a capacidade preditiva das ferramentas de IA, torna-se imprescindível o desenvolvimento e a incorporação de variáveis adicionais, a fim de se obter uma análise mais ampla e precisa. Quanto maior a quantidade de variáveis relevantes incorporadas, maior será o refinamento e ajuste da análise, propiciando, assim, a obtenção de resultados mais precisos e rigorosos;

LOE4 – Cooperar e colaborar. A implementação de protocolos de colaboração entre as diversas entidades, configura-se como medida essencial para fomentar a cooperação e a partilha de informações e dados. Além disso, o estabelecimento de relações institucionais sólidas enseja a criação de canais de comunicação técnicos diretos, fundamentais para superar eventuais limitações ou identificar e abordar áreas problemáticas. Em complemento, sublinha-se que a colaboração entre entidades pode resultar no desenvolvimento de soluções tecnológicas inovadoras e na criação de sinergias.

Comtemplados todos os resultados obtidos nesta investigação, salienta-se que uma das limitações da investigação passou pela impossibilidade de, na recolha de dados através de inquérito por entrevista ao Comando da GNR, não ter sido possível obter diferentes perspetivas dos vários níveis de comando. Todavia, considera-se que a investigação reúne contributos sólidos e úteis, tendo por base

um estudo credível e sustentado, do qual resultam propostas concretas, que se considera acrescentarem valor ao conhecimento sobre a temática.

Finalmente, como estudos futuros, e decorrente dos dados obtidos da Questão n.º 10 dos inquéritos por entrevista, sugere-se uma nova linha de investigação que incida na possibilidade do MOPREVIS poder adaptar-se a outras áreas de natureza preventiva, como por exemplo aos incêndios rurais.

REFERÊNCIAS BIBLIOGRÁFICAS

Alastruey, C. F. (2021). Estado de la cuestión de la inteligencia artificial y los sistemas de aprendizaje autónomo. *Sociology and Technoscience*, *n.º 11*, 182-195.

Alves, A. C. (2008). *Em busca de uma Sociologia de Polícia*. Lisboa: Edição da Revista da Guarda Nacional Republicana.

ANSR. (2018). *Relatórios de Sinistralidade*. Retirado de ANSR: http://www.ansr.pt/Estatisticas/RelatoriosDeSinistralidade/Pages/default.aspx

Bryman, A. (2012). *Social research methods (Fourth edi)*. United Kingdom: Oxford University Press.

Carapeto, C., & Fonseca, F. (2014). *Administração Pública. Modernização, Qualidade e Inovação*. Lisboa: Edições Sílabo.

Chand, A.; Jayesh, S.; Bhasi, A. B. (2021). Road traffic accidents: An overview of data sources, analysis techniques and contributing factors. *Materials Today: Proceedings, Volume 47, Part 15*, 5135-5141.

Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Information Management, vol 60*, 1-17.

Comissão Europeia. (2020). *Livro Branco sobre a inteligência artificial - Uma abordagem europeia virada para a excelência e a confiança*. Bruxelas.

Costa, J.; Jacques, M.; Pereira, P.; Freitas, E.; Soares, F. (2018). Portuguese two-lane highways: modelling crash frequencies for different temporal and spatial aggregation of crash data. *Transport, vol. 33*, 92-103.

Decreto-Lei n.º 2/2019, de 11 de janeiro. (2019). *Institui o Sistema Nacional de Monitorização e Comunicação de Risco, de Alerta Especial e de Aviso à População*. Diário da República n.º 8/2019, Série I,105-108. Lisboa: Presidência do Conselho de Ministros.

Despacho n.º 10393/2010, de 05 de maio. (2010). *Aprova o novo Regulamento Geral do Serviço da Guarda Nacional Republicana*. Diário da República, 2.ª série,

N.º 119, 33856 -33891. Lisboa: Comando Geral.

Domínguez, J. A. (2019). *Manual de Investigación de Siniestros Viales*. Mérida: Dirección General de la Guardia Civil - Dirección General de Tráfico.

Educação Rodoviária. (s.d.). *A História e Evolução do Automóvel em Portugal* [Online]. Retirado de http://educacaorodoviaria.pt/lazer/85-a-historia-e-evolucao-do- automovel-em-portugal

European Commission. (2021). *European Road Safety Observatory - Annual statistical report on road safety in the EU 2020*. Brussels: European Commission, Directorate General for Transport.

Eurostat. (2021). *Road Accidents: Number of Fatalities Continues Falling* [Online]. Retirado de https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/ddn- 20210624-1

Fachada, C. P., Ranhola, N. M., Marreiros, J. P., & Santos, L. A. (2020). *Normas de Autor no Instituto Universitário Militar (3.ª ed.)*. Pedrouços: Centro de Investigação e Desenvolvimento do Instituto Universitário Militar.

Freixo, M. J. (2012). *Metodologia Científica, fundamentos métodos e técnicas (4a Edição)*. Lisboa: Instituto Piaget.

Guarda Nacional Republicana. (1997). *Manual de Operações, vol II*. Lisboa: CEGRAF/GNR.

Guedelha, M. J. (Coord.) (2020). *Estratégia da Guarda 2025, uma estratégia centrada nas pessoas*. Lisboa: GNR.

Gutierrez-Osorio, C., & Pedraza, C. (2020). Modern data sources and techniques for analysis and forecast of road accidents: A review. *Journal of Traffic and Transportation Engineering*, 432-446.

Halim, Z., Kalsoom, R., Bashir, S., & Abbas, G. (2016). Artificial intelligence techniques for driving safety and vehicle crash prediction. *Artificial Intelligence Review,* 351-387.

Helm, J. M., Swiergosz, A. M., Haeberle, H. S., Karnuta, J. M., Schaffer, J. L., Krebs, V. E., Ramkumar, P. N. (2020). Machine Learning and Artificial Intelligence: Definitions, Applications, and Future Directions. *Current Reviews in Musculoskeletal Medicine,* 69-76.

Hill, M. M., & Hill, A. (2016). *Investigação por Questionário*. Lisboa: Edições Sílabo.

Hossain, M.; Abdel-Aty, M.; Quddus, M. A.; Muromachi, Y.; Sadeek, S. N. (2019). Realtime crash prediction models: State-of-the-art, design pathways and ubiquitous requirements. *Accident Analysis and Prevention, vol 124*, 66-84.

Humphrey, A. (2005). SWOT analysis for management consulting. *SRI alumni Newsletter*, 1, 7-8.

Infante, P., Afonso, A., Jacinto, G., Rego, L., Nogueira, P., Silva, M., Rebelo, P. (2022c). Some Determinants for Road Accidents Severity in the District of Setúbal. *Springer Proceedings in Mathematics & Statistics, vol 398,* 1-12.

Infante, P., Jacinto, G., Afonso, A., Rego, L., Nogueira, P., Silva, M., Manuel, P. R. (2022b). Comparison of Statistical and Machine-Learning Models on Road Traffic Accident Severity Classification. *Computers,* 1-12.

Infante, P., Jacinto, G., Afonso, A., Rego, L., Nogueira, P., Silva, M., Manuel, P. R. (2023a). Factors That Influence the Type of Road Traffic Accidents: A Case Study in a District of Portugal. *Sustainability, 15, 2352,* 1-16.

Infante, P., Jacinto, G., Santos, D., Nogueira, P., Afonso, A., Quaresma, P., Manuel, P. R. (2023b). Prediction of Road Traffic Accidents on a Road in Portugal: A Multidisciplinary Approach Using Artificial Intelligence, Statistics, and Geographic Information Systems. *Information 14, no. 4:* 238, 1-18.

Infante, P., Nogueira, V., Manuel, P. R., Góis, P., Afonso, A., Santos, D., ... Clemente, R. (2022a). *A Sinistralidade Rodoviária no Distrito de Setúbal* [versão PDF]. Évora: Imprensa da Universidade de Évora.

IUM. (2020a). *NEP/INV – 0 1– Procedimentos Relativos à Elaboração de Trabalhos de Investigação no Âmbito de Cursos que não Atribuem Grau Académico*. Lisboa: Instituto Universitário Militar.

IUM. (2020b). *NEP/INV – 03 – Estrutura e Regras de Citação e Referenciação de Trabalhos Escritos a Realizar no Instituto Universitário Militar*. Lisboa: Instituto Universitário Militar.

Leal, A. J. (2016). Sinistralidade rodoviária: métodos de estudo das causas e causas conhecidas. *Pela Lei e Pela Grei n.º 112,* 23-37.

Lei n.º 63/2007, de 06 de novembro. (2007). *Aprova a orgânica da Guarda Nacional Republicana*. Diário da República, 1.ª série, n.º 213, 8043-8051. Lisboa: Assembleia da República.

Likert, R. (1932). *A technique for the measurement of attitudes*. Retirado de Archives of Psychology, 140, 44-53. Retirado de https://legacy. voteview .com/pdf/Likert_1932.pdf

Management Solutions. (2018). *Machine-Learning, uma peça-chave na transformação dos modelos de negócio*. Espanha: MSO.

Marcillo, P., Caraguay, Á. L., & Hernández-Álvarez, M. (2022). A Systematic Literature Review of Learning-Based Traffic Accident Prediction Models Based on Heterogeneous Sources. *Applied Sciences,* 1-27.

Moraes, B. B. (2005). *Prevenção criminal ou conivência com o crime: uma análise brasileira*. São Paulo: Revista dos Tribunais.

Nogueira, P., Silva, M., Infante, P., Nogueira, V., Manuel, P., Afonso, A., Gois, P. (2023). International journal og Geo-Information. *Learning from Accidents: Spatial Intelligence Applied to Road Accidents with Insights from a Case Study in Setúbal District,* Portugal, 1-14.

Organização Mundial de Saúde. (2004). *A Segurança Rodoviária não é Acidental* [*Online*]. Retirado de WHO: https://apps.who.int/iris/bitstream/handle/10665/68500/WHO_NMH_VIP_03.4_por.pdf

Organização Mundial de Saúde. (2021). *Plano Global - Década de Ação pela Segurança no Trânsito 2021-2030*. WHO.

Pérez, M. R. (2011). ¿Se debe usar el término accidente en el ámbito de la investigación científica? *Panace@. Vol. XII, n.o 33. Primer semestre*, 84-88.

Racioppi, F., Eriksson, L., Tingvall, C., & Villaveces, A. (2004). *Preventing Road Traffic Injury: a Public Health Perspective for Europe*. Copenhaga: WHO.

Raimundo, A., & Sebastião, P. (2021). *Novos Modelos de Negócio com Recurso à Inteligência Artificial* [*Online*]. Retirado de https://www.iapmei.pt/PRODUTOS-E-SERVICOS/Empreendedorismo-Inovacao/Empreendedorismo-(1)/DOCS_Emp/Novos-modelos-de-negocio-com-recurso-a-Inteligenci.aspx

Resolução do Conselho de Ministros n.º 85/2017, de 19 de junho. (2017). *Plano Estratégico Nacional de Segurança Rodoviária - PENSE 2020*. Diário da República n.º 116/2017, Série I. Lisboa: Presidência do Conselho de Ministros.

Santos, D., Saias, J., Quaresma, P., & Nogueira, V. B. (2021). *Computers. Machine Learning Approaches to Traffic Accident Analysis and Hotspot Prediction,* 1-5.

Santos, L. A., & Lima, J. M. (Coords.) (2019). *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação* - Caderno n.º 8 (2.ª edição, revista e atualizada). Lisboa: Instituto Universitário Militar.

Silva, P.B.; Andrade, M.; Ferreira, S. (2020). Machine learning applied to road safety modeling: A systematic literature review. *Journal of Traffic Transportation Engineering (Engl. Ed.), vol 7*, 775-790.

Sousa, A. F. (2003). Prevenção e Repressão como Função da Polícia e do Ministério Público. *Revista do Ministério Público n.º 94*, 49-63.

Stobierski, T. (2019). *What is Statistical Modeling For Data Analysis?* [*página online*]. Retirado de Northeeastern University Graduate Programs: https://www.northeastern.edu/graduate/blog/statistical-modeling-for-data-analysis/

Tabasso, C. (2012). *Paradigmas, teorías y modelos de la seguridad y la inseguridad vial [Documento eletrónico]*. Retirado de http://94.23.80.242/~aec/ivia/tabasso_124.pdf UNISDR. (2009). Terminology on Disaster Risk Reduction [Online]. Retirado de https://www.unisdr.org/files/7817_UNISDRTerminologyEnglish.pdf

Universidade de Évora. (s.d.). *MOPREVIS [página online]*. Retirado de Modelação e Prediçao de Acidentes de Viação no Distrito de Setúbal: https://moprevis.uevora.pt/ Yannis, G., Dragomanovits, A., Laiou, A., Richter, T., Ruhl, S., Torre, F. L.,Li, H. (2016). Use of accident prediction models in road safety management – aninternational inquiry. Transportation Research Procedia n.º 14, 4257-4266.

Zaal, D. (1994). *Traffic Law Enforcement: A review of the literature, Report No. 53*. Australia: Monash University Accident Research Centre.

Os **Cadernos do IUM** têm como principal objetivo divulgar os resultados da investigação desenvolvida no/sob a égide do IUM, autonomamente ou em parcerias, que não tenha dimensão para ser publicada em livro. A sua publicação não deverá ter uma periodicidade definida. Contudo, deverão ser publicados, pelo menos, seis números anualmente. Os temas devem estar em consonância com as linhas de investigação prioritárias do CIDIUM. Devem ser publicados em papel e eletronicamente no sítio do IUM. Consideram-se como objeto de publicação pelos Cadernos do IUM:

- Trabalhos de investigação dos investigadores do CIDIUM ou de outros investigadores nacionais ou estrangeiros;
- Trabalhos de investigação individual ou de grupo de reconhecida qualidade, efetuados pelos discentes, em particular pelos do CEMC e pelos auditores do CPOG que tenham sido indicados para publicação e que se enquadrem no âmbito das Ciências Militares, da Segurança e Defesa Nacional e Internacional;
- *Papers*, ensaios e artigos de reflexão produzidos pelos docentes;
- Comunicações de investigadores do IUM efetuadas em eventos científicos (e.g., seminários, conferências, *workshops*, painéis, mesas redondas), de âmbito nacional ou internacional, em Portugal ou no estrangeiro.

N.os Publicados:

1 – Comportamento Humano em Contexto Militar
Subsídio para um Referencial de Competências destinado ao Exercício da Liderança no Contexto das Forças Armadas Portuguesas: Utilização de um "Projeto STAfS" para a configuração do constructo

Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

2 – Entre a República e a Grande Guerra: Breves abordagens às instituições militares portuguesas

Coordenador: Major de Infantaria Carlos Afonso

3 – A Abertura da Rota do Ártico (*Northern Passage*). Implicações políticas, diplomáticas e comerciais

Coronel Tirocinado Eduardo Manuel Braga da Cruz Mendes Ferrão

4 – O Conflito da Síria: as Dinâmicas de Globalização, Diplomacia e Segurança
(Comunicações no Âmbito da Conferência Final do I Curso de Pós-Graduação em Globalização Diplomacia e Segurança)

Coordenadores: Tenente-coronel de Engenharia Rui Vieira
Professora Doutora Teresa Ferreira Rodrigues

5 – Os Novos Desafios de Segurança do Norte de África

Coronel Tirocinado Francisco Xavier Ferreira de Sousa

6 – Liderança Estratégica e Pensamento Estratégico
Capitão-de-mar-e-guerra Valentim José Pires Antunes Rodrigues

7 – Análise Geopolítica e Geoestratégica da Ucrânia
Coordenadores: Tenente-coronel de Engenharia Leonel Mendes Martins
Tenente-coronel Navegador António Luís Beja Eugénio

8 – Orientações Metodológicas para a elaboração de Trabalhos de Investigação
Coordenadores: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos
Tenente-coronel Técnico de Manutenção de Material Aéreo Joaquim Vale Lima

9 – A Campanha Militar Terrestre no Teatro de Operações de Angola. Estudo da Aplicação da Força por Funções de Combate
Coordenadores: Coronel Tirocinado José Luís de Sousa Dias Gonçalves
Tenente-coronel de Infantaria José Manuel Figueiredo Moreira

10 – O Fenómeno dos *"Green-on-Blue Attacks"*. *"Insider Threats"* – Das Causas à Contenção
Major de Artilharia Nelson José Mendes Rêgo

11 – Os Pensadores Militares
Coordenadores: Tenente-coronel de Engenharia Leonel José Mendes Martins
Major de Infantaria Carlos Filipe Lobão Dias Afonso

12 – *English for Specific Purposes* no Instituto Universitário Militar
Capitão-tenente ST Eling Estela do Carmo Fortunato Magalhães Parreira

13 – I Guerra Mundial: das trincheiras ao regresso
Coordenadores: Tenente-coronel de Engenharia Leonel José Mendes Martins
Major de Infantaria Fernando César de Oliveira Ribeiro

14 – Identificação e caraterização de infraestruturas críticas – uma metodologia
Major de Infantaria Hugo José Duarte Ferreira

15 – O DAESH. Dimensão globalização, diplomacia e segurança. Atas do seminário 24 de maio de 2016
Coordenadores: Tenente-coronel de Engenharia Adalberto José Centenico
Professora Doutora Teresa Ferreira Rodrigues

16 – Cultura, Comportamento Organizacional e *Sensemaking*
Coordenadores: Coronel Piloto Aviador João Paulo Nunes Vicente
Tenente-coronel Engenheira Aeronáutica Ana Rita Duarte Gomes S. Baltazar

17 – Gestão de Infraestruturas Aeronáuticas
Major Engenheira de Aeródromos Adelaide Catarina Gonçalves

18 – A Memória da Grande Guerra nas Forças Armadas
Major de Cavalaria Marco António Frontoura Cordeiro

19 – Classificação e Análise de Fatores Humanos em Acidentes e Incidentes na Força Aérea
Alferes Piloto-Aviador Ricardo Augusto Baptista Martins
Major Psicóloga Cristina Paula de Almeida Fachada
Capitão Engenheiro Aeronáutico Bruno António Serrasqueiro Serrano

20 – A Aviação Militar Portuguesa nos Céus da Grande Guerra: Realidade e Consequências
Coordenador: Coronel Técnico de Pessoal e Apoio Administrativo
Rui Alberto Gomes Bento Roque

21 – Saúde em Contexto Militar (Aeronáutico)
Coordenadoras: Tenente-coronel Médica Sofia de Jesus de Vidigal e Almada
Major Psicóloga Cristina Paula de Almeida Fachada

22 – *Storm Watching. A New Look at World War One*
Coronel de Infantaria Nuno Correia Neves

23 – Justiça Militar: A Rutura de 2004. Atas do Seminário de 03 de março de 2017
Coordenador: Tenente-coronel de Infantaria Pedro António Marques da Costa

24 – Estudo da Aplicação da Força por Funções de Combate - Moçambique 1964-1975
Coordenadores: Coronel Tirocinado de Infantaria Jorge Manuel Barreiro Saramago
Tenente-coronel de Infantaria Vítor Manuel Lourenço Ortigão Borges

25 – A República Popular da China no Mundo Global do Século XXI. Atas do Seminário de 09 de maio de 2017
Coordenadores: Professora Doutora Teresa Ferreira Rodrigues
Tenente-coronel de Infantaria Paraquedista Rui Jorge Roma Pais dos Santos

26 – O Processo de Planeamento de Operações na NATO: Dilemas e Desafios
Coordenador: Tenente-coronel de Artilharia Nelson José Mendes Rêgo

27 – Órgãos de Apoio Logístico de Marinhas da OTAN
Coordenador: Capitão-tenente de Administração Naval Duarte M. Henriques da Costa

28 – Gestão do Conhecimento em Contexto Militar: O Caso das Forças Armadas Portuguesas
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

29 – A Esquadra de Superficie da Marinha em 2038. Combate de alta Intensidade ou Operações de Segurança Marítima?
Capitão-de-mar-e-guerra Nuno José de Melo Canelas Sobral Domingues

30 – Centro de Treino Conjunto e de Simulação das Forças Armadas
Coronel Tirocinado de Transmissões Carlos Jorge de Oliveira Ribeiro

31 – Avaliação da Eficácia da Formação em Contexto Militar: Modelos, Processos e Procedimentos
Coordenadores: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro
Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

32 – A Campanha Militar Terrestre no Teatro de Operações da Guiné-Bissau (1963-1974). Estudo da Aplicação da Força por Funções de Combate
Coordenadores: Brigadeiro-general Jorge Manuel Barreiro Saramago
Tenente-coronel de Administração Domingos Manuel Lameira Lopes

33 – O Direito Português do Mar: Perspetivas para o Séc. XXI
Coordenadora: Professora Doutora Marta Chantal Ribeiro

8 – Orientações Metodológicas para a elaboração de Trabalhos de Investigação (2.ª edição, revista e atualizada)
Coordenadores: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos
Coronel Técnico de Manutenção de Material Aéreo Joaquim Vale Lima

34 – Coreia no Século XXI: Uma península global
Coordenadores: Professora Doutora Teresa Ferreira Rodrigues
Tenente-coronel Rui Jorge Roma Pais dos Santos

35 – O "Grande Médio Oriente" Alargado (Volume I)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Ricardo Dias Costa

36 – O "Grande Médio Oriente" Alargado (Volume II)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Ricardo Dias Costa

37 – As Forças Armadas no Sistema de Gestão Integrada de Fogos Rurais
Coordenador: Tenente-coronel Rui Jorge Roma Pais dos Santos

38 – A Participação do Exército em Forças Nacionais Destacas: Casos do Kosovo, Afeganistão e República Centro-Africana. Vertente Operacional e Logística
Coordenadores: Brigadeiro-general Jorge Manuel Barreiro Saramago
Major de Transmissões Luís Alves Batista
Major de Material Tiago José Moura da Costa

39 – Pensar a Segurança e a Defesa Europeia. Atas do Seminário de 09 de maio de 2019
Coordenador: Tenente-coronel Marco António Ferreira da Cruz

40 – Os Desafios do Recrutamento nas Forças Armadas Portuguesas. O Caso dos Militares Contratados
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

41 – Inovação na Gestão de Recursos Humanos nas Forças Armadas Portuguesas: Os Militares em Regime de Contrato. Atas das Comunicações do *Workshop* de 28 de janeiro de 2019
Coordenador: Coronel Tirocinado Lúcio Agostinho Barreiros dos Santos

42 – Sistemas de Controlo de Gestão: Modelos, Processos e Procedimentos
Coordenador: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro

43 – Desafios Estratégicos para Portugal no Pós-Covid-19
Auditores Nacionais do Curso de Promoção a Oficial General 2019/2020

44 – Gestão Estratégica: Contributos para o Paradigma Estrutural da Marinha Portuguesa
Capitão-de-mar-e-guerra Nuno Sardinha Monteiro

45 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume I)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

46 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume II)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

47 – A Geopolítica dos *Chokepoints* e das *Shatterbelts* (Volume III)
Coordenadores: Professor Doutor Armando Marques Guedes
Tenente-coronel Marco António Ferreira da Cruz

48 – Estudos Estratégicos das Crises e dos Conflitos Armados
Coordenadores: Brigadeiro-general Lemos Pires
Tenente-coronel Ferreira da Cruz
Tenente-coronel Pinto Correia
Tenente-coronel Bretes Amador

49 – A Vulnerabilidade em Infraestruturas Críticas: Um Modelo de Análise
Tenente-coronel Santos Ferreira

50 – Função de Combate Proteção
Coordenadores: Coronel de Infantaria Paulo Jorge Varela Curro
Major de Cavalaria Rui Miguel Pinho Silva

51 – Estudos Estratégicos das Crises e dos Conflitos Armados
Coordenadores: Coronel de Cavalaria (Reformado) Marquês Silva
Tenente-coronel GNR Marco Cruz
Tenente-coronel ENGEL Silva Costa
Major Engenheiro Reis Bento

52 – Reinventar as Organizações Militares
Coordenador: Tenente-coronel de Administração Militar Carriço Pinheiro

53 – Estudos de Reflexão sobre as Informações Militares
Coordenador: Tenente-coronel de Infantaria Carlos Marques da Silva

54 – Convulsões Eurasiáticas. *in illo tempore* e agora
Coordenador: Coronel (Reformado) Carlos Manuel Mendes Dias

55 – Estratégias Marítimas – Uma Análise Comparativa (NATO, UE, Espanha, França, Itália, Portugal e Reino Unido)
Coordenadora: Capitão-tenente Sofia Saldanha Junceiro

56 – Ensino e Formação, Avaliação de Desempenho e Retenção do Talento: Dimensões para o Desenvolvimento da Liderança
Coordenador: Tenente-coronel Nuno Alberto Rodrigues Santos Loureiro

57 – Ameaças Híbridas - Desafios para Portugal
Coordenador: Tenente-coronel de Artilharia Diogo Lourenço Serrão

58 – Cadernos de Saúde Militar e Medicina Operacional – Vol. I
Coordenadores: Coronel (REF) António Correia
Primeiro-tenente Nicole Esteves Fernandes

59 – *Military Operations in Cyberspace*
Coordinator: Lieutenant-colonel João Paulo Ferreira Lourenço

Editorial: cidium@ium.pt
Telefone: (+351) 213 002 100; Fax: (+351) 213 002 162
Morada: Rua de Pedrouços - 1449-027 Lisboa