Cadernos do IUM

SEGURANÇA INTERNA: FRONTEIRAS, INTELIGÊNCIA ARTIFICIAL E COMUNICAÇÃO EM CRISE

Coordenação de:
Tenente-Coronel GNR Reinaldo Saraiva Hermenegildo

IUM

Setembro 2025

INSTITUTO UNIVERSITÁRIO MILITAR

SEGURANÇA INTERNA: FRONTEIRAS, INTELIGÊNCIA ARTIFICIAL E COMUNICAÇÃO EM CRISE

Coordenador

Tenente-coronel GNR Reinaldo Saraiva Hermenegildo

IUM – Centro de Investigação e Desenvolvimento (CIDIUM)
Setembro de 2025

Como citar esta publicação:
Hermenegildo, R. S., (Coord.), (2025). *Segurança Interna: Fronteiras, Inteligência Artificial e Comunicação em Crise*. Cadernos do IUM, 67. Instituto Universitário Militar.

Diretor
Vice-Almirante José António Vizinha Mirones

Editora-chefe
Coronel Joana Isabel Azevedo do Carmo Canhoto Brás

Coordenador Editorial
Capitão-de-fragata Luís Carlos Brandão Marques

Capa – Composição Gráfica
Divisão de Comunicação e Relações-Públicas - Guarda Nacional Republicana

Propriedade e Edição
Instituto Universitário Militar
Rua de Pedrouços, 1449-027 Lisboa
Tel.: (+351) 213 002 100
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: 978-989-36168-0-2
ISSN: 2183-2129
Depósito Legal: 555056/25
Tiragem: 90 exemplares

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

PREFÁCIO

A temática da segurança interna, enquanto pilar fundamental da soberania e da estabilidade dos Estados, assume uma especial relevância no atual contexto de crescente volatilidade geopolítica, bem como perante os desafios colocados pelas novas ameaças e riscos transnacionais.

Esta edição, tendo por base trabalhos académicos, e abordando alguns casos de estudo de relevo, incentiva-nos a uma reflexão profunda sobre as problemáticas atuais da segurança interna, oferecendo uma perspetiva abrangente e atual sobre os seus principais dilemas e desafios.

Em Portugal, tal como nos demais Estados-Membros da União Europeia, a segurança interna não se limita apenas ao domínio da ordem pública ou da prevenção criminal, mas integra uma abordagem multidimensional que abrange a proteção de infraestruturas críticas, a segurança no ciberespaço, o controlo de fronteiras e a gestão integrada de crises. A globalização, a intensificação dos fluxos migratórios, a criminalidade organizada transnacional e a proliferação de ameaças assimétricas, vieram complexificar o atual ambiente securitário, exigindo a articulação entre os diversos Estados-Membros e as instâncias de cooperação europeia.

Pretende-se com esta publicação, excelentemente coordenada pelo Tenente-coronel Reinaldo Hermenegildo, apresentar oito artigos científicos que oferecem uma análise aprofundada das dinâmicas nacionais e europeias da segurança interna.

Acreditamos que todos estes artigos, sendo da responsabilidade dos seus autores, são um estimulante contributo para a partilha de conhecimento e reflexão académica através da conjunção da perspetiva teórica com estudos de caso.

IUM, 29 de agosto de 2025

Paulo Daniel Duarte Machado
Coronel Tirocinado GNR
Coordenador da AESIFC

ÍNDICE

INTRODUÇÃO GERAL

A segurança interna ganhou relevância diária nas sociedades, mas ainda não obteve o devido realce académico, sobretudo em Portugal. Embora existam estudos, nomeadamente em instituições associadas ao ensino destas atividades, estes estão, por norma, muito direcionados para o interior das organizações e, na ótica do profissional que vai participar nas atividades de segurança interna – a diferentes níveis –, e na perspetiva mais restrita da segurança interna, ou seja, na sua vertente de ação policial.

O Instituto Universitário Militar (IUM) comemora em 2025, 10 anos da sua criação, pelo que representa um marco e um processo de afirmação das ciências militares, no espetro do ensino superior. Por impulso normativo e institucional, as ciências militares passaram a integrar cinco subáreas, entre as quais os Estudos de Segurança Interna e dos Fenómenos Criminais.

Este impulso foi inédito, na medida, em que as matérias da segurança interna passaram a integrar uma das áreas nucleares das ciências militares, o que não é a regra no âmbito desta potencial área científica, ainda pouco afirmada e aprofundada.

Porém, contribuiu para abrir novos caminhos de ensino e investigação, mesmo que o seu enquadramento organizativo seja discutível – e é. Mas na realidade não foi motivo impeditivo do seu desenvolvimento.

Na prática, o legislador, também por influência da instituição militar, refletiu e tentou fazer corresponder as ciências militares, a uma lógica organizativa já consolidada do ensino superior militar ministrado nas academias, escolas e institutos das forças armadas. Porém, dois desses estabelecimentos de ensino integram, igualmente, a formação superior dos oficiais das GNR, razão pela qual foi aditada e integrada a subárea dos "estudos de segurança interna e dos fenómenos criminais".

Destarte, o que temos é uma tentativa de arrumação científica do ensino ministrado, que embora discutível, contribuiu para que esta área de estudo de potencial científico possa ser estudada no espetro académico, no quadro do ensino superior militar, que embora não se limite, nem deva, limitar a este, mas sem este, porventura, ficaria ainda mais deficitário e fragmentado o seu ensino e investigação.

Esta transformação permitiu que o ensino da segurança interna passasse a ser ministrado aos alunos da Guarda Nacional Republicana (GNR) na Academia Militar, numa primeira fase; e noutra fase, aos alunos da GNR que frequentam o curso de promoção a oficial superior no IUM, até então, ainda focado na vertente

mais policial e na ótica do interveniente e não tanto da compreensão e de pensamento critico sobre estas temáticas.

Assim, estas alterações permitiram contribuir para melhor compreender, explicar e pensar do ponto de vista científico a segurança interna, nomeadamente as suas principais problemáticas e desafios.

É nesta lógica, que damos à estampa o resultado produzido, no âmbito da Unidade Curricular – Estudos de Segurança Interna, ministrada no ano letivo 2024/25 (1.ª ed) de um conjunto de estudos de encimado valor, que se interligam umbilicalmente com a linha programática da Unidade Curricular, em especial as suas problemáticas atuais.

A obra *Segurança Interna: Fronteiras, Inteligência Artificial e Comunicação em Crise* contempla, a presente introdução, em guisa de enquadramento dos estudos que a procedem. Um primeiro estudo de Reinaldo Saraiva Hermenegildo, intitulado *Pensar a segurança interna em tempo de liberdade e alucinação*, na qual o autor procura efetuar uma reflexão sobre a emergência e evolução concetual da segurança interna e a sua dificuldade de delimitação. No ensaio é explorada a pouca atenção que as matérias de segurança interna tiveram pela Academia, contrariamente à importância que a atividade tem nas sociedades.

Umbilicalmente relacionado com o texto anterior, o trabalho de Cátia Tomás, apresenta um debate constante de equilíbrio e desafios decorrente do processo de integração europeia e o exercício da soberania, no âmbito de um domínio, com uma tendência supranacional, mas com caraterísticas intergovernamentais, como podemos constatar em *Frontex e a soberania nacional: Desafios e Implicações para os Estados-membros da União Europeia*, na qual a autora, em parte baseada na sua experiência profissional, desenvolve de forma equilibrada e adequada a investigação desta temática atual.

João Romano, procura através do conflito Rússia-Ucrânia perscrutar como este se refletiu na segurança interna da União Europeia (UE), nomeadamente da crise dos deslocados. Desta abordagem é percetível compreender que a segurança interna não é exercida apenas no plano nacional, mas também no domínio europeu e esta está interdependente da vertente externa e carece da coordenação de vários intervenientes, seja por uma questão de interesse dos Estados ou de compromisso humanitário, conforme é discutido em *Reflexos do conflito Rússia-Ucrânia na segurança interna da União Europeia - da crise dos deslocados*.

André Barreira, em *A Segurança Interna na Quarta Revolução Industrial: Oportunidades e Desafios*, discute e conclui que a segurança interna se confronta

com um novo paradigma operativo, no qual as tecnologias emergentes oferecem diversas oportunidades a serem exploradas para melhorar a eficácia e eficiência das operações. Todavia, existam limitações, que devem ser tidas em conta, nomeadamente, uma integração coordenada das soluções tecnológicas nas mudanças organizacionais, sendo essencial uma abordagem crítica e responsável à sua implementação.

O estudo de Pedro Costa, *Inteligência Artificial no Policiamento Preditivo: Análise e Prevenção de Crimes*, explora a forma como a Inteligência Artificial (IA) tem contribuído para transformar os modelos tradicionais de atuação policial, através do desenvolvimento de estratégias preditivas baseadas em dados. O autor conclui que a IA representa uma mais-valia na eficiência policial e na gestão estratégica de recursos. Porém, a sua implementação exige um quadro legal robusto, transparência e salvaguarda dos direitos fundamentais.

Em *Videovigilância com Inteligência Artificial na União Europeia: pertinência e enquadramento*, de João Carreiro é-nos apresentada uma investigação da conjuntura atual das tecnologias de videovigilância integradas com IA na UE e a abordagem sobre o papel crescente da IA nos sistemas de vigilância e reflexão sobre os limites éticos e legais da sua implementação, estabelecendo um foco quase transversal na tensão entre segurança pública e direitos fundamentais, na qual conclui que, embora a IA associada a sistemas de videovigilância contemple benefícios evidentes para a segurança, a UE adota uma abordagem cautelosa e regulatória, diferenciando-se do modelo mais permissivo dos Estados Unidos da América e do autoritarismo digital chinês.

Sara Vale, problematiza *O papel da Inteligência Artificial na Investigação Criminal*, avaliando as suas potencialidades, limitações e desafios no contexto contemporâneo da segurança interna, na qual evidência como a IA representa uma ferramenta transformadora para as atividades de prevenção criminal e investigação criminal. A autora, conclui que, apesar do seu potencial transformador, a utilização da IA na investigação criminal deve ser acompanhada por um escrutínio rigoroso e de um enquadramento legal adequado que salvaguarde os valores democráticos.

Por fim, João Lourenço, desenvolve a sua investigação sobre *A comunicação em situações de crise nas Forças de Segurança*, com o objetivo de compreender de que modo a comunicação em situações de crise pode influenciar a perceção de legitimidade de atuação pelos próprios polícias. O autor baseia o seu estudo em dois casos mediáticos, na GNR e na Polícia de Segurança Pública, que permitiram analisar e explorar a resposta institucional e o seu efeito mediático, na qual concluiu

que a comunicação em situações de crise desempenha um papel relevante para garantir o posicionamento das forças de segurança na esfera pública.

Assim, este trabalho concatenado em *Segurança Interna: Fronteiras, Inteligência Artificial e Comunicação em Crise*, pretende contribuir para a discussão da segurança interna, das suas problemáticas e desafios, bem como lançar eixos renovados de investigação científica. Nessa medida, é necessário continuar este caminho de aquisição e procura do conhecimento científico, ancorado na "curiosidade", na liberdade de pensamento, no rigor, na discussão de ideias inovadoras, da continuidade e consistência na investigação, e naturalmente de recursos humanos motivados, competentes em qualidade e quantidade. Sem pelos menos estes ingredientes, não haverá domínio científico que se (a)firme.

O Coordenador

Reinaldo Saraiva Hermenegildo
Tenente-coronel GNR
Professor e Coordenador Científico no IUM
Investigador IPRI-NOVA

ESTUDO 1 – PENSAR A SEGURANÇA INTERNA EM TEMPO DE LIBERDADE E ALUCINAÇÃO

RETHINKING INTERNAL SECURITY IN A TIME OF FREEDOM AND DELUSION

Reinaldo Saraiva Hermenegildo
Tenente-coronel GNR
Professor e Coordenador Científico no IUM
Investigador IPRI-NOVA

RESUMO

O presente estudo analisa criticamente o conceito de segurança interna e a sua evolução histórica, a partir de uma abordagem interdisciplinar, ancorada sobretudo na lente das relações internacionais. Discute-se a falta de uma matriz teórica própria e coerente, o que dificulta a afirmação da segurança interna como campo científico autónomo.

O trabalho destaca a influência de acontecimentos marcantes, como os atentados de 11 de setembro de 2001, e a evolução política, normativa e institucional da União Europeia, na reconfiguração do conceito, gradualmente marcado por uma crescente complexidade, assente em matrizes e lógicas cruzadas, e caraterizado pela intervenção de múltiplos atores, tanto a nível infra como supraestatal, para responder a um conjunto diversificado e alargado de ameaças, riscos e fontes de insegurança.

Conclui-se que, embora a segurança interna assuma uma progressiva centralidade nas agendas políticas e académicas, continua desprovida de um enquadramento teórico estável e coerente, o que dificulta a sua compreensão, explicação e predição a nível científico.

Palavras-chave: segurança interna; segurança nacional; União Europeia; matriz teórica; ambiguidade concetual.

ABSTRACT

This study critically analyses the concept of internal security and its historical evolution, based on an interdisciplinary approach, anchored above all in the field of international relations. It discusses the lack of its own coherent theoretical framework, which hinders the recognition of internal security as an autonomous scientific field.

The work highlights the influence of landmark events, such as the attacks of 11 September 2001, and the political, normative and institutional evolution of the European Union, on the reconfiguration of the concept. This redefinition is inncreasingly marked by growing complexity,

shaped by intersecting frameworks and logics, and characterised by the involvement of multiple actors, both at the infra- and supra-state levels, in responding to a diverse and extensive range of threats, risks and sources of insecurity.
The study concludes that, although internal security has assumed growing prominence on political and academic agendas, it still lacks a stable and coherent theoretical Foundation, which complicates its scientific understanding, explanation, and prediction.

***Keywords**: internal security; national security; European Union; theoretical framework; conceptual ambiguity*

1. PROLEGÓMENOS

É possível que nunca tenhamos tido tantos instrumentos à nossa disposição para expressar o exercício da liberdade como temos atualmente. No entanto, acabamos por ficar ancorados a um tempo, sem tempo, porque vivemos alucinados, ou seja, sem liberdade. Ora esta alucinação, que as tecnologias e particularmente a inteligência artificial vieram estimular, acelerar e exponenciar, nem sempre tem contribuído para uma reflexão e sistematização do conhecimento, nomeadamente no domínio da segurança interna, uma vez que "é cada vez mais evidente a escassa utilidade de velhos instrumentos concebidos para espaços delimitados e para tempos lentos e sincronizáveis" (Innerarity, 2021, p. 16). Também, porventura, nunca se falou tanto de segurança (interna), existindo mesmo uma "paixão pela segurança nas sociedades europeias" (Editorial comments, 2024), criando a ideia de um estado de "insegurança permanente" ou de "normalização do Estado de exceção", em nome da "guerra" contra o terrorismo, a Covid-19 (Brouillet, 2023, pp. 9-10) e os afluxos migratórios. Porém, sem se balizar corretamente o que é, e, muito menos, sem a definição de uma matriz teórica que sistematize e estribe, o que é, e não é; mas acima de tudo que contribua para a sua compreensão, explicação e previsão.

As matérias de segurança exigem um reexame analítico e concetual constantes, dado que vão impactar na forma como a segurança é ensinada, pensada e praticada (Balzacq, 2003-2004, pp. 33-34), sobretudo dada a complexidade crescente das dinâmicas políticas, que implicam um estudo constante, para uma desejável sintonia entre a teoria e a prática. A procura de quadros explicativos, balizados cientificamente, que nos facultem instrumentos de interpretação, compreensão e explicação da realidade, seja esta mais constante ou volátil, é uma variável presente em todos os domínios científicos. No campo da segurança assume uma necessidade

premente e constante, dadas as frequentes mutações da realidade e a dificuldade, também dai adveniente, em estancar determinadas variáveis, para poder estudar um determinado fenómeno.

Ao estudar as matérias de segurança existe, por vezes, uma confusão, ao misturar o objeto de estudo, com a área científica que se procura ancorar a investigação de uma problemática, o que pode conduzir a um enviesamento da análise, sobretudo, se feita com o recurso a metodologias nem sempre apropriadas para o efeito.

O estudo da segurança decorre de tentativas de explicação do fenómeno securitário, que surgiram no quadro das teorias das relações internacionais, e desde a sua génese foi um conceito "essencialmente contestado", que associado à plasticidade do termo "segurança" (Balzacq, 2003-2004, p. 34), aplicado, por vezes, em vários domínios de forma diferenciada, não contribuiu para a sua clareza explicativa, mantendo um caráter ambíguo.

O aparecimento das matérias de segurança na agenda de investigação de relações internacionais está associado à evolução do seu próprio domínio científico e dos seus paradigmas. As preocupações do Estado sempre estiveram ligadas à segurança – a necessidade de segurança está na sua génese e a esta é fundamental à existência do Estado. Contudo, estas sofreram alterações, que conduziram a uma necessidade maior de compreender este fenómeno específico no quadro das relações internacionais, dando origem a escolas de pensamento da segurança, que derivam das próprias teorias das Relações Internacionais. Necessidade essa, que foi também paralela, nas agendas políticas dos governos ocidentais.

Nessa medida, podemos compreender, que mesmo um conceito, em que existiam estudos científicos para o tentar compreender e explicar, e uma necessidade prática e política para a sua compreensão, as tentativas de definição de segurança, nunca esteve isenta de riscos, não tanto pela sua inserção nos domínios da vida social, mas sobretudo, por ser um conceito conotado ideologicamente (Balzacq, 2003-2004, p. 34; *Editorial comments*, 2024), pelo que procurar no passado recente tentativas de explicação do conceito de segurança (interna) é um exercício anacrónico e pletórico.

No caso da segurança interna ainda estamos perante uma complexidade maior, dado que esta enquanto atividade, de forma gradual, ganhou uma relevância maior. Mas, por outro lado, o seu estudo foi sendo disseminado, de forma *ad hoc* e sem um perfil formativo e de investigação, nem sempre coerente, ministrado em diferentes

cursos ou sob o jugo de áreas científicas diferenciadas, em que "com abordagens metodológicas diversificadas têm proporcionado recortes variados destes objetos de tão difícil delimitação e análise" (Gonçalves, 2012, p. 714), que apesar de contribuir, para compreender determinados acontecimentos, não nos permite um compressão global da segurança interna, dada a carência de uma grande teoria ou um quadro abrangente (Kiltz & Ramsay, 2012, p. 3; Comiskey, 2018, 29-45).

As preocupações centrais dos Estados, mesmo após o final da guerra-fria, eram sobre segurança, sendo que a academia acompanhou também essa linha de preocupação, procurando explicar o que era a segurança, em que ganharam proeminência a Escola de Copenhaga e, posteriormente, de Paris. Mas o foco, era na segurança, compreender o que tinha mudado e que tentativas de explicação existiam, que afetavam o Estado e que ameaças de origem externa colocavam em causa a segurança do Estado. Nesse sentido, apesar do alargamento e aprofundamento do conceito de segurança e do aparecimento do domínio da "segurança interna" nessas escolas de pensamento, nomeadamente através da Escola de Paris, no início da década de 90, esta não ganhou primazia equivalente na academia.

A nível interno, os problemas eram de outra natureza e consequência – internos, e, por regra, circunscritos a determinadas áreas do território (a capital), ou seja, de ordem pública que afetavam a ordem e a estabilidade política dos governos.

Nesta perspetiva, falar em segurança interna, antes da década de 80, é um exercício difícil de deslindar. Por motivos de vária ordem, mas interligados. Em primeiro lugar, a falta de estruturas institucionais e quadro normativo específico de segurança interna. A conceção de segurança interna, embora parcamente estudada, ainda na atualidade, não é transponível, com evidência, para o passado. O que temos são áreas de intervenção segmentadas e recortadas, que hoje, as catalogamos como atividades de segurança interna. Mas, nesta fase, por definição e natureza a segurança interna (ou conceções análogas e interdependentes, embora mais restritas, como ordem pública e segurança pública) eram poderes do Estado.

O objetivo do presente estudo é compreender e explicar a evolução do conceito de segurança interna e como esta se interliga com a dificuldade e necessidade de criar um quadro teórico específico, que contribua para a definição, compreensão, explicação e predição científica da segurança interna.

Assim, o presente ensaio está organizado da forma seguinte: os prolegómenos, onde é introduzida a problemática concetual acerca da segurança interna; no primeiro ponto, enquadramos os eixos fundamentais da emergência

e desenvolvimento da segurança interna; no segundo ponto, discorremos acerca da evolução teórica e necessidade do seu estudo e investigação; em terceiro lugar, levantamos um conjunto de questões e desafios de investigação, em torno do conceito e modelo teórico; terminamos, com as conclusões.

2. A EMERGÊNCIA DA SEGURANÇA INTERNA E DO SEU ESTUDO

As preocupações e a necessidade do estudo da segurança interna foram feitas, sobretudo, após o 11 de setembro de 2001, e, pela via da explicação da então "nova" segurança e da interdependência, entre o interno e o externo, na lógica da Escola de Paris. Embora tenha emergido de forma segmentada em relação a uma temática – o terrorismo, sobretudo nos EUA, e cumulativamente, numa tentativa de abordagem concetual e teórica (White, 2018), que difere, das potenciais conceções europeias, no primeiro caso como uma abordagem intermédia e inferior, mas bastante lata, entre a segurança nacional tradicional – função exclusiva do Estado em que ameaça principal é externa –, e a visão clássica europeia em que a segurança interna era sobretudo atividade de polícia e de ordem pública, impregnada numa tradição político-administrativa fundada sobre um Estado forte, nomeadamente nos países em que têm um modelo de origem francesa (Malochet, 2021a).

Também, pelo seu curto período nas agendas políticas, a segurança interna encontra-se ainda despojada de estudos científicos – de (grande) profundidade e continuidade, e cumulativamente de uma matriz teórica que escore toda uma explicação racional.

Encontramos estudos parcelares, alguns de cariz institucional ou com fortes ligações e influência deste; outros constituem capítulos de outras áreas científica, desde o direito, a criminologia, a sociologia, a ciência política, as relações internacionais, a história, entre outras. Contudo, carecem de uma matriz teórica, que congregue perspetivas de várias ciências de forma a contribuir para uma explicação sustentada e estribada em alicerces científicos sólidos.

Assim, o que temos atualmente é sobretudo uma explicação de segmentos, atividades ou eventos catalogados de segurança interna explicados à luz de diferentes áreas científicas, que se por um lado, a enriquecem enquanto abordagem multidisciplinar; noutra perspetiva, é o reflexo da sua fragilidade, em especial, porque os estudos não conseguem ter uma visão coerente, integrada e unificadora, em parte, porque estão ávidos de um quadro teórico específico.

Constitui-se como paradoxal, que uma atividade que sempre existiu, pelo menos, desde a criação do Estado moderno, embora com outras denominações e numa perspetiva mais restrita, que não tenha merecido um olhar e análise atenta dos cientistas, mas apenas seja sujeita a explicações parcelares, fragmentadas, e, por vezes, justificativas de um determinado contexto ou como resposta desconexa a um problema público circunscrito.

Também não deixa de suscitar perplexidade o facto de esta ter começado a merecer mais atenção a nível académico, quando emergiu no plano europeu uma dimensão de segurança interna, ou seja, quando esta se tornou relevante "fora" e "acima" do Estado, mas com os Estados (Hermenegildo, 2013, 2016, 2017, 2024).

Nos EUA, o termo segurança interna (*Homeland Security*) passou a ser usado com regularidade no léxico político, académico e nos média, apenas após o 11 de setembro de 2001. A ameaça terrorista conduziu ao desenvolvimento e criação de programas, agências e políticas destinadas a proteger o país, nomeadamente a uma profunda reorganização, que levou à criação do *Department of Homeland Security*, resultante da fusão de 22 agências federais distintas (Kiltz, & Ramsay, 2012, p. 2).

Também no continente europeu, a situação foi similar, a expressão segurança interna apareceu tardiamente nos textos legislativos. No caso francês, por exemplo, surge no Decreto-lei de 91/903, de 10 de setembro de 1991, de organização do Instituto de Altos Estudos de Segurança Interna, criado em 1989. Sendo que a expressão foi finalmente retomada, com a Lei n.º 2002/1094, de 28 de outubro de 2002, relativa à orientação e programação da segurança interna; e com a reativação do Conselho de Segurança Interna, criado em 1986, após os atentados de outono desse ano, na dependência do Primeiro-ministro, mas que ficou "congelado", sendo reativado e passado para a dependência do Presidente da República, em 2002 (Heyeghe, 2018; Doaré et Frustié, 2019, p. 20; Palo, 2021; Brouillet, 2023, p. 1).

No caso português, a primeira referência é feita na Lei n.º 30/84, de 5 de setembro – *Lei-Quadro do Sistema de Informações da República Portuguesa*, mas sem se definir o que é segurança interna. Sendo que a primeira Lei de segurança interna (Lei n.º 20/87, de 12 de junho), embora apresente a definição de segurança interna[1], o objetivo principal desta foi, em articulação com o documento anterior,

[1] "A segurança interna é a actividade desenvolvida pelo Estado para garantir a ordem, a segurança e a tranquilidade públicas, proteger pessoas e bens, prevenir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos e liberdades fundamentais dos cidadãos e o respeito pela legalidade democrática." (artigo 1,º , n.º 1).

integrar o novo Serviço de Informações e Segurança, no catálogo de forças e serviços de segurança interna.

Porém, essa introdução e normalização do termo na linguagem quotidiana não foi acompanhada por uma discussão científica do mesmo (Pelfrey & Kelley, 2013; White, 2018; Comiskey, 2018; Dahl & Ramsay, 2024). Inicialmente o conceito de segurança interna surge, em geral, como sinónimo dos esforços nacionais para prevenir a ameaça terrorista e minimizar a vulnerabilidade dos EUA, no caso de um ataque ocorrer. Posteriormente, esta conceção *monolítica*, com Obama, foi alargada, para incluir outras ameaças e riscos (por ex. catástrofes naturais); bem como outros atores a diferentes níveis – federal, estatal, local; e de natureza – privados, não-governamentais, com um interesse comum no bem-estar e segurança pública dos EUA; e mais tarde fundiu o conceito de segurança nacional com o de segurança interna (Estratégia de Segurança Nacional – 2010). Desta forma, na conceção institucional americana, a segurança interna passou para um conceito abrangente, passando a incluir a defesa civil, resposta a emergências, aplicação da lei, controlo das fronteiras e imigração (Kiltz, & Ramsay, 2012, pp. 2-9).

Assim, a ligação entre segurança nacional e segurança interna ou a noção de segurança global, para proteger os interesses de um Estado no interior ou no exterior é feita, quando a lente de análise é das relações internacionais (Kiltz, & Ramsay, 2012, p. 9; Comiskey, 2018, pp. 29-45). Por sua vez, quando se procura analisar segmentos da segurança interna, ou seja, a tendência é o recurso à ótica do direito (Berthelet, 2016; Palo, 2021; Dupin, 2024), criminologia (Cusson, 2007, 2014; Chetrit, 2012) ou da sociologia (Roché, 2004; Malochet, 2018, 2021a, 2021b; Malochet et Ocqueteau, 2020).

Esta metamorfose do conceito e a dificuldade do seu estudo propiciou também um debate acerca da putativa discussão sobre a autonomia da segurança interna, enquanto área científica – que não se consolidou; em parte porque o próprio conceito, não se estabilizou, não sendo possível encontrar um padrão e consenso concreto, por esse motivo, não sendo considerada uma disciplina.

Embora existam estudos, que procuram sustentar que a segurança interna no ciclo de vida de evolução de uma disciplina é uma área científica "jovem" e no início da fase de emergência (Falkow, 2013)[2]. Contudo, segundo Pelfrey e

[2] O autor recorre a uma escala de referências das disciplinas, em que: 0-20% (não é uma disciplina académica; 20%-40% (potencial de disciplina académica); 40%-60% (jovem/disciplina académica em emergência); 60%-80% (disciplina académica matura); 80%-100% (disciplina plenamente académica). A segurança interna, neste estudo obteve 41,34% (Falkow, 2013, pp. 74-75).

Kelley (2013, p. 8), apesar da sua evolução, não foram criadas teorias ou métodos idiossincráticos de investigação específicos; nem é garantido, que estes sejam mais adequados do que os modelos de outras áreas científicas que estudam a segurança interna. Por outro lado, a formação na área da segurança interna parece "imatura e amorfa", pelo que é pouco suscetível de criar programas além dos que fornecem os conhecimentos e as competências necessárias aos responsáveis que já desempenham funções definidas de segurança interna e posições-chave de segurança pública. Nesse sentido, de acordo com os mesmos autores, nesta fase, o mais adequado é capitalizar o desenvolvimento das necessidades imperativas da segurança interna e de investigação no âmbito das disciplinas existentes, construindo assim uma base sólida para uma disciplina mais madura da segurança interna (Pelfrey e Kelley, 2013, p. 8).

Mas, noutra perspetiva, pode ser catalogada como uma meta-disciplina, porque a segurança interna não encaixa em nenhum modelo, mas engloba várias disciplinas, com natureza interdisciplinar, e deve ser vista mais como uma "disciplina prática", como a medicina, a engenharia ou o direito, com uma forte ligação entre a academia e os profissionais da segurança interna (Pelfrey & Kelley, 2013; White, 2018; Dahl & Ramsay, 2024).

No plano europeu e no passado recente, a segurança interna, podia ser entendida como um conjunto de atividades desenvolvidas no seio de um Estado soberano, tendo em vista a manutenção da ordem e tranquilidade pública, o assegurar do cumprimento e do respeito pelas leis no interior de um Estado, a salvaguarda da legalidade democrática e o livre exercício de funções das instituições democráticas (Hermenegildo, 2016). Conceito este, bem como a definição normativa da lei de segurança interna portuguesa[3], carece de ser revisto, dado que, no plano europeu, a segurança interna não se circunscreve apenas, a uma dimensão estatal, embora, ainda só exista, com este; e no plano interno, assistimos a uma pluralização e hibridação da lógica dos atores de segurança interna (Maillard, 2010, pp. 57-77; Heyeghe, 2018, pp. 52-53; Renaudie, 2018, pp- 53-66; Malochet, 2021a, 2021b), por vezes, a funcionar de forma fragmentada, e em "silos", sem uma verdadeira organização e coordenação entre eles, que tem conduzido à necessidade de uma recomposição interna dos atores e a uma necessidade de reforço da organização e

[3] N.º 1, do artigo 1.º, Lei N.º 53/2008, de 29 de agosto. Apesar da Lei já ter sofrido 10 alterações, a definição de segurança interna manteve-se inalterada, apesar de alguns ajustes nos fins e princípios.

da coordenação (Brodeur, 2010; Icard, lemaire et Maillard, 2024), bem como a uma alteração concetual, de *continuum* de segurança, para "segurança global" (Thourot et Fauvergue, 2018).

A segurança interna foi assim, recuperar elementos da segurança pública (ordem e tranquilidade pública), da criminalidade (prevenção e repressão), de proteção (catástrofes, riscos) e da segurança (defesa) em sentido lato e clássico (ameaças externas e militares), muitas vezes confundindo-se ou fundindo-se (Chetrit, 2012; Palo, 2021).

Na linha de White, a segurança interna engloba ações destinadas a proteger uma nação de uma destruição catastrófica interna (White, 2018). Por sua vez, para Morag (2011), é realmente um "sistema de sistemas" que engloba uma série de campos aparentemente díspares que partilham um objetivo comum: a manutenção da segurança pública, a estabilidade da sociedade e da economia e, mais importante ainda, a continuidade do governo.

Por outro lado, para Icard, lemaire e Maillard (2024), por detrás de uma definição simples – a proteção dos indivíduos contra ataques deliberados à sua propriedade ou integridade física – o conceito de segurança combina aspetos diferentes e potencialmente contraditórios: fenómenos objetivos e sentimentos subjetivos; dimensões internas e externas (uma distinção que resulta da formação histórica dos Estados e da consolidação das fronteiras estatais); abordagens preventivas (entendidas como todas as ações não coercivas tomadas contra as causas do crime com o objetivo específico de reduzir a probabilidade ou a gravidade do crime) e abordagens repressivas (baseadas na definição e aplicação de sanções) (Icard, lemaire et Maillard, 2024).

Já para Maurice Cusson (2014, p. 7) e Pascal Brouillet (2023), a segurança interna só pode ser definida pela sua finalidade – gerir a violência, com o objetivo de garantir a segurança e a paz social. Nessa medida, longe de ser um conceito claro e operacional, seria, portanto, uma noção ou uma série de ações destinadas a estabelecer a possibilidade de viver em paz numa determinada área.

Pese embora, as tentativas ora referidas, o termo é um *contradictio in adjecto* – uma vez que a segurança consiste na condição – de estar seguro. Por sua vez, a segurança interna é apresentada, como ação e dirigida para o interior do território. Ou seja, estamos perante um duplo oxímero, uma vez que, o termo, representa condição e ação. Nesse sentido, o conceito de segurança interna surge com uma roupagem de um "acontecer-fazer e não apenas como um estado ou condição"

(Fernandes, 2011, p. 71). Por outro lado, com o acrescento da expressão "interior", quando esta não existe apenas e circunscrita ao interior de um Estado[4].

A nível metodológico, afigura-se um exercício difícil – estudar um fenómeno que aparentemente se modificou, sem primariamente existiram estudos – estabilidade – do que é esse mesmo fenómeno. Ou seja, quando os estudos são incrementados já o conceito se encontra desajustado, o que revela um longo hiato, entre a realidade e a sua explicação, e, por conseguinte, o seu uso operativo.

Embora todos compreendam intuitivamente a que se refere o termo segurança interna, o conceito é recente e vago, abrangendo muitas realidades. Poder-se-á, assim, pensar que o conceito é oco, logo inútil, até mesmo perigoso, pois a falta de uma definição clara pode justificar eventuais excessos (Brouillet, 2023).

Desta forma, a noção de segurança interna evoluiu em função dos perigos e das ameaças a que o Estado e a sociedade estão expostos. Desde a sua recente e tardia aparição, tornou-se um conceito completo a nível político e administrativo, mas paradoxalmente complexo, dado que, apesar da sua utilização recorrente, não é fácil definir legalmente os seus contornos, devido à ausência de uma definição e à constante evolução da realidade (Chetrit, 2012, p. 9; Brouillet, 2023).

Em Portugal, a raridade de estudos científicos, além de parcos, pecam pela pouca profundeza, consistência, estruturação e continuidade de análise. A esse facto, não deixa de ser alheio a não existência de centros de investigação especializados, com corpo de investigadores academicamente qualificados e especializados; bem como, poucas linhas de investigação desenvolvidas em diversos centros de investigação.

Por outro lado, alguns dos textos, sobre estas matérias são de elementos das forças e serviços de segurança, o que conduz muitas vezes a uma perspetiva pouco imparcial, com pendor corporativo, levando a uma putativa diminuição de credibilidade. Deste conjunto, ainda se verifica, por vezes, uma constante, de que estes se considerarem os únicos detentores do conhecimento e informação sobre matéria de segurança interna (Debove et Renaudie, 2013, p. VIII). Ora este facto, é um indicador evidente da falta de conhecimento destes sobre estas matérias e da complexidade que enferma a compreensão da evolução das problemáticas que esta engloba.

---

[4] Contudo, nos países anglo-saxónicos, "«National Security»/«Security» não significam somente uma condição a assegurar ou objetivo a atingir; também querem dizer ação, implementação de medidas" (Dias & Sequeira, 2015, p. 125).

Estudar fenómenos particulares ou setoriais, da atividade de segurança interna, mesmo sob diferentes ângulos científicos, apesar de enriquecedor, para a compreensão desse fenómeno particular, não representa o estudo da segurança interna (do conjunto), embora possa contribuir para esse.

Volvidos mais de 10 anos da aprovação do Tratado de Lisboa que contribuiu para um salto significativo na evolução da segurança interna, no plano europeu, com consequências nos Estados-membros, na qual derrogou algumas das suas competências e ou implicou que estes alterassem o seu quadro normativo e organizativo (Verdelhan, 2024; Places, 2024), nomeadamente em Portugal, na qual resultou a implementação e evolução do atual sistema de segurança interna, o seu arquétipo legislativo e operacional, importa efetuar uma reflexão profunda, sistematizada, com base científica, acerca deste período, para poder contribuir para um diagnóstico e debate, tendo em vista uma melhoria do sistema, em consonância, com a evolução que os quadros operacionais, concetuais e normativos tiveram.

O Tratado de Lisboa trouxe uma nova forma de governação das matérias de segurança interna, ao criar o Espaço de Liberdade, Segurança e Justiça (ELSJ) num domínio genericamente comunitário, mas mantendo e até incrementando medidas, ações e matérias de natureza interestadual, embora, *sui generis*, dado persistirem traços de intergovernamentalidade, uma vez que os Estados continuam a ter um papel central, embora partilhado com a Comissão (Brandão, 2016, 2022; Hermenegildo, 2017, 2024). Assim, assistimos, a uma reconceptualização da segurança e da segurança interna, por força do direito da UE.

Contudo, o Tratado, também reconheceu que a ordem e a segurança pública são fundamentais para a soberania, como reconhece o artigo 4.º, n.º 2, do Tratado da União Europeia (TUE) e, na verdade, os artigos 72.º e 346.º do Tratado sobre o Funcionamento da União Europeia (TFUE). Os Estados-membros continuam a ser Estados neste sentido, a perseverar os seus valores, identidades e continuam a ser os principais responsáveis pela ordem e segurança pública. Estes aspetos não foram substancialmente alterados pelos desenvolvimentos recentes, apesar de modificar o quadro de atuação, em áreas centrais dos seus poderes soberanos, decorrente da europeização deste domínio, e do papel primariamente complementar da UE –, mas que, ainda não está na fase de fornecer segurança diretamente, em termos operacionais, com a possível exceção da FRONTEX (Hermenegildo, 2018; Places, 2024; Coutts, 2024, pp. 1482-1485).

O artigo 72.º do TFUE – constitui uma salvaguarda (dos interesses dos Estados-membros), mas esta não exclui o âmbito de aplicação do direito da UE, no cômputo da implementação das medidas nacionais, para efeitos de aplicação e de manutenção da ordem ou da segurança interna; esta disposição tem duas funções. Em primeiro lugar, serve como um *lembrete* das responsabilidades das instituições da UE. Como tal, obriga, *inter alia*, a UE a garantir que os instrumentos do ELSJ deixam uma possibilidade genuína para os Estados-membros os exercerem. Em segundo lugar, poderia também, teoricamente, justificar que os Estados-membros se afastassem dos instrumentos do ELSJ em determinadas "circunstâncias excecionais" (Thym, 2021; Verdelhan, 2024). No entanto, apesar da tendência crescente do Tribunal de Justiça da UE (TJUE) se pronunciar sobre questões de segurança e do conflito de aplicação de normas – em geral associadas a matérias do domínio digital e das migrações –, entre o nacional e europeu, ainda carece de definição precisa do que é segurança, segurança interna, segurança e ordem pública e termos como "circunstâncias excecionais".

Assim, resulta que os Estados continuam a ser os principais responsáveis por garantir a ordem pública e a definir a política de segurança, mas os seus poderes são reformulados e controlados por novas fórmulas de legislação da União, a qual desde o início da década de noventa e de forma crescente, deixou de ter apenas um papel regulatório sobre os Estados-membros, passando a ter competências que tocam diretamente nas funções essenciais do Estado; por outro lado, os Estados, dada a multiplicidade de ameaças e de incerteza têm procurado assegurar os interesses coletivos, através da União, para se manterem "soberanos" (Coutts, 2024, pp. 1475-76).

Apesar da relutância dos Estados, em por vezes, aceitarem esta transformação ou reinterpretarem parcialmente o direito da UE e os padrões preconizados pelo TJUE, no âmbito deste domínio, como ocorreu em França, na qual o Conselho de Estado, em 21 de abril de 2021, no caso *French Data Network*, não seguiu a interpretação do TJUE, especialmente a estabelecida em *Digital Rights Ireland, Tele2 Sverige e La Quadrature du Net*, que proibia a retenção generalizada e indiscriminada de dados. Mas criou uma exceção constitucional interna vaga baseada na segurança nacional, permitindo a continuidade da recolha e retenção massiva de dados, com base no artigo 4.º, n.º 2 do TUE, para justificar a segurança nacional como parte da identidade constitucional francesa, o que permitiria afastar obrigações da UE (Turmo, 2024).

Nesse sentido, os Estados tendencialmente aparentam ter mais dificuldades em reconhecer as competências da UE neste domínio, por esta ser uma matéria sensível e com previsão ambígua nos tratados, mas preferem dar primazia ao *soft law* e práticas informais, materializadas, nomeadamente numa forte dimensão operacional da segurança interna europeia, dado aparentemente refletir o ressurgimento do poder do Estado (Berthelet, 2016, pp- 352-354).

De forma paralela, nos últimos 20 anos, a nível interno, assistimos a mutações consideráveis das condições de produção de segurança interna para além do Estado, nomeadamente a uma diversificação e recomposição dos atores, traduzida numa pluralização, fragmentação e heterogeneidade de dinâmicas. Mas, por outro lado, a um crescimento e centralização do controlo hierárquico dentro das forças policiais de natureza estadal (Icard, lemaire et Maillard, 2024, pp. 7-12), em que estas ainda consideram o modelo centralizado como um "paradigma irreversível" (Malochet, 2021a, p. 2).

O domínio da segurança interna tornou-se mais difuso, complexo, indefinido, antes da sua própria definição e estabilização. Sendo neste quadro que evoluiu: no plano externo, para um sistema binário mesclado, entre o comunitário e o intergovernamental, em que ambos se cruzam, rompendo com modelos clássicos, hierarquizados, verticalizados, padronizados e hermeticamente balizados; no plano interno, para uma pluralidade de atores, de diferente natureza – pública (nacional e local) e privados, *semi* público-privados; com funções privadas exercida por agentes públicos, e atividades tradicionalmente públicas por elementos privados. Se acrescentáramos a esta evolução, a sua evolução material: primeiro, próximo ou equivalente a segurança pública (ordem e tranquilidade, função de polícia); depois, adicionada a criminalidade (e o incremento da sua severidade), por fim, dimensão de proteção/segurança civil (catástrofes, riscos naturais).

No caso português, em especial, assistimos a um modelo de segurança interna de origem francesa – centralizado, vertical e dual (forças de segurança de natureza militar e policial), complementado por uma multiplicidade de atores, sobreposto com um modelo de segurança interna da União, de influência alemã, de natureza supranacional, multinível e em rede.

Assim, atualmente, temos dois modelos de segurança interna cruzados, coordenados pelo sistema de segurança interna, que progressivamente foi ganhando áreas funcionais e competências, de coordenação e articulação dos atores, a nível nacional e internacional.

3. ACERCA DO MODELO TEÓRICO E CONCETUAL

Apesar da relevância da atividade de segurança interna no quotidiano do cidadão e da complexidade da gestão política desta área setorial, desde logo pela "dupla pressão securitária e orçamental" (Malochet et Ocqueteau, 2020) e por novas formas de *accountabilty* (Heyegh, 2018, 17), a mesma está desprovida de estudos científicos, nomeadamente em Portugal. Nesse sentido, importa, tentar compreender, algumas das razões e lógicas cruzadas, que contribuíram para o seu caráter perfuntório no espetro académico. Assim, apresentamos algumas das possíveis razões:

(1) A não existência de uma área científica própria que estude as matérias que engloba. Os estudos existentes resultam, sobretudo, de estudos de domínios científicos que "olham" para a segurança interna como estudo de caso e fenómenos particulares, e não, um domínio a estudar de forma continua e consistente.

(2) Relacionada com a anterior, carência de centros de investigação que estudem a atividade e os diversos fenómenos de segurança interna, mas sobretudo, investigadores que se dediquem ao estudo sustentado e continuado deste campo de investigação, mesmo através do olhar de outro domínio científico.

(3) O facto de no geral não existir um sentimento generalizado de insegurança, e a inexistência de ameaças constantes, que afetem o quotidiano das populações.

(4) Há uma maior preocupação com a atividade em si e uma resposta imediata a problemas específicos de determinado tipo de fenómenos, em vez de se proceder a uma análise das causas e a um estudo para melhorar o sistema.

(5) Textos de intervenientes na segurança interna, sobre acontecimentos particulares, sem escrutínio académico e ou base científica.

(6) Ensino monogâmico da segurança interna, com caráter reduzido de abertura.

(7) Diminuta, embora crescente, comunidade científica, em Portugal. No plano europeu, verifica-se uma tendência de incremento do estudo da segurança interna, decorrente do reforço do reforço do ELSJ; bem como, nos EUA, desde o 11 de setembro de 2001, embora, este movimento não tenha sido linear.

O cenário que vivemos em Portugal, não difere significativamente de outros países, com exceção sobretudo, de países como a França e Inglaterra, em que associado a um maior desenvolvimento científico geral e a um conjunto de ameaças constantes ao país, tem desenvolvido uma panóplia mais vasta de estudos, apesar de que se comparada com a prática, a teoria está subdesenvolvida (Cusson, 2014, p. 1).

Destarte, o que tem contribuído de forma mais proeminente para o estudo da segurança interna foi o facto da sua crescente importância e de esta ter transbordado o domínio nacional, para o plano europeu, que trouxe consigo o despertar do interesse pela comunidade científica, em especial da ciência política, das relações internacionais e do direito. Assim, atualmente existem mais estudos sobre a segurança interna europeia (Bossong and Rhinard, 2012; Hermenegildo 2013, 2017; Brandão, 2016, 2022), do que sobre a segurança interna (no plano nacional), como entendida genericamente e normativamente.

Esse facto conduziu a que o estudo da segurança interna fosse absorvido pelos "estudos europeus", passando a ser uma área de análise do ponto de visto teórico e vibrante no plano político, porque é uma síntese e reflexo do processo de integração europeia, bem como de um eterno debate entre Estado-soberano e integração europeia.

O transbordo da segurança interna do domínio nacional coloca em causa parcelas nucleares do Estados, que estes encaram como centrais do seu círculo soberano e raio fundamental de ação da política interna. Contudo, apesar de a segurança interna ultrapassar a dimensão estático-centrica, continua ancorada ao Estado e a ter como eixo central as forças de segurança. No entanto, a associação tradicional e, na verdade, a convergência entre o Estado, o exercício da força, a definição e a garantia da ordem pública e da segurança pública foram reestruturadas no âmbito da mudança do quadro normativo da União (Dupin, 2023; Coutts, 2024, p. 1475; *Editorial Comments*, 2024, pp. 285-295).

Com efeito, faz sentido a existência do termo segurança interna? Se sim, quais são os parâmetros que a delimitam? A segurança interna existe apenas (ou sobretudo) no domínio nacional? A atividade e por inerência o conceito extravasou o campo nacional, logo é coerente usar o sintagma "segurança interna", quando o interno ficou desprovido de significado? Ou é interno no que respeita ao território e jurisdição europeia? A segurança interna abarcou e ultrapassou a própria segurança nacional, de onde emergiu? A falta de consenso do conceito e a não existência de uma dimensão preditiva (estratégia) a nível interno (Estados), mas

a nível europeu deve-se a que? Podemos ter previsão (estratégia) se não temos estabilizado o conceito, ou seja, a compreensão?

A segurança interna surgiu ontologicamente da necessidade de segurança do Estado, e não da proteção de pessoas e bens (Debove et Renaudie, 2013, p. XI), ou seja, da conceção ambígua de segurança nacional (Balzacq, 2003-2004; Coste, 2011; Crawford, 2014). Esta premissa refletiu-se na organização das Policias, com duas consequências: Estado ocupa um papel preponderante e centralizador. Foi assim, que a Polícia foi pensada e implementadas as políticas públicas, em França, e posteriormente, nos países europeus, que seguiram o modelo francês (Debove et Renaudie, 2013, p. XI; Malochet, 2021b, p. 2), como foi o caso de Portugal. As forças de segurança eram a extensão administrativa e a presença política do Estado central em todo o território (em especial as de natureza militar), por vezes, mais importante a presença, para segurança do Estado, do que para a segurança das populações (Renaudie, 2018, p. 62).

Esta reconfiguração do papel do Estado e por inerência da segurança interna trouxe desafios de eficácia, de qualidade e de proximidade (Heyeghe, 2018, pp. 55-58), sobretudo, em tempos em que a segurança interna extravasou o domínio nacional e perante a tendência maior e incontornável do avanço tecnológico. Estes fenómenos, em parte, desvirtuaram a lógica ontológica da segurança interna – presença e proximidade do Estado em todo o território nacional.

O surgimento do modelo tradicional, embora com diferenças, dos países do sul da Europa (França, Espanha, Portugal e Itália) tem a sua origem remota ao aparecimento do Estado moderno, em 1648, através da criação da *liutenante de police* em Paris, a 15 de março de 1667. Inicialmente o papel da polícia era predominantemente de garantir a ordem pública. Essencialmente, depois da segunda guerra mundial, este papel começou a abarcar outras áreas de atuação, decorrente das preocupações de insegurança, associadas à delinquência e a um ressentimento de insegurança, na qual deu origem ao repensar do então modelo policial tradicional e a uma globalização das respostas à insegurança (Debove et Renaudie, 2013, p. XI; Heyeghe, 2018, p. 49) e ao aparecimento de novos formatos de policiamento, na qual a sociologia deu um contributo importante.

Porém, as preocupações com a segurança interna, surgem na agenda política, de forma muito tardia, após o final dos anos de 1980, essencialmente, acantonadas à delinquência. Até esse período, que coincidiu com o período da guerra-fria, as preocupações eram de segurança do Estado, e não dentro do

Estado. O fator guerra ocupa, ainda, as preocupações centrais dos Estados, no que concerne à agenda de segurança. Embora, a partir dos anos de setenta, inúmeros trabalhos tenham destacado a erosão progressiva do papel do Estado em matéria de segurança, na qual Roché (2004), qualificou como um processo de "desmonopolização das funções soberanas", dada a crescente pluralidade de atores – públicos e privados, envolvidos nas questões de segurança e de prevenção da delinquência (Icard, Lemaire, Maillard, 2024, p. 24).

Na década de setenta e oitenta, o surgimento da delinquência juvenil, sobretudo nas grandes áreas urbanas, como em França trouxeram um sentimento de insegurança, que este tipo de criminalidade ou de incivilidades provocavam em algumas regiões (Chetrit, 2021), tendo conduzido a um conjunto de programas de policiamento e a novas tarefas para as forças de segurança, que ultrapassavam até então, a sua principal preocupação e atividade – a ordem pública, na qual se inicia um ciclo, para a emergência da segurança interna, ainda recortada e limitada, se comparada com as áreas que gradualmente passou a englobar.

Com o 11 de setembro de 2001, o discurso político de segurança é centralizado na ameaça terrorista, bem como no conjunto de ameaças difusas, reais ou supostas, ligadas à globalização, que destruiu as fronteiras e fez emergir perigos. É neste período que a clássica distinção entre segurança interna e defesa se torna desajustada. Não se tratou apenas de uma modificação do sentido dos termos, mas de uma inadequação do vocabulário de segurança (Brouillet, 2013, p. 3; Heyeghe, 2018, pp. 49-ss), que conduziu, progressivamente a um alargamento e interconexão, sem critério objetivo, com outras áreas setoriais (energia, saúde, criminalidade, comunicações, migração, segurança rodoviária, entre outros) (*Editorial comments*, 2024) e ao incremento da heterogeneidade do conceito de segurança (Crawford, 2014).

Nessa medida, os acontecimentos de 11 de setembro de 2001, trouxeram para a agenda pública de decisão, as matérias de segurança, nomeadamente de segurança interna, com reflexo incontornável no seu conceito e modelos. Este tipo de fenómeno – terrorismo, pela escala, impacto e amplo grau de visibilidade conduziu a que os Estados olhassem para a segurança interna, como "um assunto de todos" (Debove et Renaudie, 2013, p. XII).

Esta discussão foi feita em França, mas também na generalidade dos países europeus e em Portugal (Teixeira, 2006; Lourenço 2006), na qual se refletiu na forma de encarar este domínio, em que os Estados têm a responsabilidades primária

em matéria de segurança interna, mas não têm mais o seu monopólio (Debove et Renaudie, 2013, p. XII), dado que este deixou de ser um dos seus "domínios reservados"; em parte, também associado a um movimento de pluralização do *policing* (Malochet, 2023), em que esta dinâmica de mudança foi igualmente afirmada nos discursos, e muito na lógica da Escola de Paris, sobe os rótulos de "coprodução" ou de "*continuum* da segurança" (Thourot, Fauvergue, 2018; Icard, Lemaire, Maillard, 2024, p. 8) "segurança partilhada" (Melchior, 1999) e de "segurança de todos" (Malochet, 2024), "ecossistema de segurança", "direito à segurança" "a segurança é a primeira das liberdades" (*Editorial comments*, 2024, p. 285), "nexo segurança interna-externa" (Eriksson e Rhinard, 2009; Trauner, 2013), "segurança interna globalizada" (Bornet, 2022) entre outros.

Nesse sentido, a forma de resolver este problema consistiu em coordenar e envolver as ações de todos os intervenientes que concorrem para a sua produção: forças policiais, poder local, magistrados, segurança social, segurança privada, entre outros. Sendo através desta conceção, que os modelos policiais evoluíram para uma maior atenção às populações e uma melhor proteção das pessoas e bens (Debove et Renaudie, 2013, p. XII), e assim, a segurança interna surge como um dos temas maiores do debate público, para a qual muito contribuíram o terrorismo e, mais tarde, as migrações.

Assistimos, assim, a uma evolução do que antecedeu a própria conceção de segurança interna, em que as preocupações da Polícia eram garantir a ordem pública, para no período posterior à II Guerra Mundial, passar a incluir outras preocupações de segurança, como seja a delinquência, mas sem grande relevância. Neste período as preocupações eram com a segurança dos Estados e não com a segurança dentro do Estado. Entre a década de setenta e finais de década de oitenta, os problemas de delinquência ganham relevância na agenda política, bem como o surgimento da ameaça terrorista, ainda que localizada, contribuíram para o surgimento de uma preconceção de segurança interna, que teve a sua afirmação e emergência, com o 11 de setembro de 2001, em que a segurança passou a ser entendida com um "assunto de todos" (Brouillert, 2013; Debove et Renaudie, 2013; Héritage, 2018)[5].

[5] O termo foi usado pelo Ministro do Interior francês, Daniel Vaillant, no âmbito do debate da lei n.º 2001-1062, de 15 de novembro de 2001, relativo à segurança quotidiana (*Cit*. Héritage, 2018, p. 48).

Esta clarificação da segurança interna também se deu, pela distinção, em relação à segurança externa, como matéria de defesa do território nacional, contra eventuais ameaças militares (Debove et Renaudie, 2013, p. XII).

Estas alterações, perceções e compreensão trouxeram consigo uma mudança de paradigma, que foi a passagem de preocupações com a "ordem" para a "segurança". Ou seja, até este período, os Estados estavam sobretudo focados na manutenção da ordem pública e não em problemas e de espetro mais lato de segurança ou do seu inter-relacionamento. Já existiam problemas setoriais de insegurança, devido a diferentes delitos e crimes, mas em geral, vistos de forma fragmentada e particular, dentro de um território, primeiro local, depois nacional, e não, de problemas de insegurança, que se interligavam, de criminalidade "multicausal" (Chetrit, 2012), nomeadamente entre a vertente externa e interna, na qual a Escola de Paris, veio dar contributos significativos, para a sua explicação.

O monopólio do Estado é desafiado, por baixo, como evidenciaram os estudos de Virgine Malochet (2023) – que qualificou de pluralização do *policing*. Mas também, por cima, pelos benefícios, embora com implicações no seu raio de ação soberana, pela UE (Hermenegildo, 2017, 2024), pelo facto do ELSJ estar enquadrado numa das doze áreas de competência partilhada, e pelo papel desenvolvido, no quadro supranacional, pelas agências Justiça e Assuntos Internos (JAI), em que estas têm um protagonismo cada vez maior (Leyen, 2024), nomeadamente a FRONTEX e a EUROPOL.

Assistimos, igualmente, a uma europeização das conceções de segurança e de ordem pública, não no sentido de restringir (negativamente) as formulações nacionais, mas positivamente, como forma de procurar uma maior legitimidade das escolhas nacionais (Coutts, 2024; Muller, 2024; Places, 2024). Até porque a conceção de segurança no direito da UE foi influenciada pelas conceções nacionais de segurança, nomeadamente pela noção francesa de segurança (Dupin, 2023, p. 20).

Ou seja, temos o aparecimento de novos atores e a reconfiguração dos tradicionais. Nessa medida, temos de analisar o seu contexto, para procurar explicar as mutações do possível conceito de segurança (interna), para tentar reduzir a sua ambiguidade (Coutts, 2024; Muller, 2024). Embora, este conceito seja por si e ao longo dos tempos eivado de ambiguidade e inconsistência, e assim, impossível de definir com neutralidade (Smith & Acharya, 2002 Balzacq, 2003-2024).

Nessa medida, o atual conceito normativo está desajustado, dado que a atividade de segurança interna não é apenas desenvolvida pelo Estado, mas também, por outros atores, no plano supra e infra estadual.

Embora, a realidade de segurança interna seja óbvia, o conceito é bem menos evidente (Cusson, 2014, p. 1). A complexidade em definir segurança interna (Chetrit, 2012, p. 760; Palo, 2021), inclusive, do ponto de vista normativo, é patente também no extenso Código de Segurança Interna francês, em que estabelece os princípios da segurança interna, mas sem definir o que é segurança interna. Nesse enquadramento, designa o primeiro capítulo de segurança pública, em que refere a importância da segurança, os princípios orientadores permanentes da segurança pública, e no capítulo segundo, refere os princípios orientadores da segurança civil.

O código de segurança interna francês apresenta a segurança interna como um conceito que abrange a proteção da população, das instituições, do território e dos interesses nacionais contra ameaças de origem interna ou externa, como o terrorismo, a criminalidade organizada, as perturbações graves da ordem pública e outras formas de violência ou risco que afetam a coesão e estabilidade do Estado.

Todavia, o artigo L111-1 do Código de Segurança Interna estabelece que "a segurança é um direito fundamental e uma das condições para o exercício das liberdades individuais e coletivas. O Estado tem o dever de garantir a segurança em todo o território da República, respeitando as liberdades e os direitos fundamentais. A política de segurança interna tem como objetivo garantir, no território nacional, a paz, a segurança e a proteção das pessoas, dos bens e das instituições."

No entanto, não é fornecida uma definição clara e concisa de segurança interna. Deve-se, portanto, deduzir que todos sabem exatamente o que é segurança em geral e segurança interna em particular (Brouillet, 2023).

Por outro lado, ainda temos o conceito de segurança pública, como entendido nos sistemas jurídicos modernos – mais concreto do que o conceito de segurança – este mais contestado, e como função central, e até a *raison d'être* do Estado (*cit*. Couts, 2024, p. 1476), mas que em algumas realidades é sinónimo de segurança interna (ex. Canadá) e outras é confundido ou usado de forma indiferenciado (Coste, 2011; Places, 2024).

Também, a exportação académica e institucional para outros contextos, do conceito de *homeland security,* concebido na perspetiva e lógica dos EUA, pós 11 de setembro, revelou-se inadequado para países de pequena e média dimensão, onde a distinção entre segurança interna e externa é, na maioria dos casos, artificial (Greene, 2022), e por consequência, gerou para uma maior confusão pública do termo, que se, por um lado expessa uma aparente carga de intelectualidade e sonoridade mediática, acaba por ter uma utilidade reduzida, dado a diferença de realidades sociais, políticas, normativas e institucionais, em relação aos Estados europeus.

Também, no plano europeu, o Tribunal de Justiça da UE procurou fazer alguma distinção, entre os conceitos de segurança nacional, segurança interna, segurança pública. Embora, se mantenham fronteiras muito ténues, por vezes cruzadas e sobrepostas, entre ambas, nomeadamente entre segurança interna e segurança nacional.

Nessa medida, a segurança nacional é da exclusiva responsabilidade de cada Estado-membro. Ou seja, Isso significa que cada país tem autonomia para definir e adotar medidas para proteger a sua soberania contra ameaças graves (ex. defesa contra ataques militares; contraespionagem e proteção de informações sensíveis; luta contra ameaças à ordem constitucional (ex.: terrorismo interno, insurreições). No entanto, o TJUE reconhece que a segurança nacional pode justificar derrogações ao direito da UE, mas apenas dentro dos limites do princípio da proporcionalidade. Mas, não podem deixar de aplicar o direito da UE[6].

Assim, para este, a segurança interna está ligada à proteção da ordem pública, à prevenção e repressão de crimes graves e à salvaguarda das instituições e da estabilidade dos Estados-membros (ex. terrorismo e crime organizado transnacional; cibercriminalidade e ameaças híbridas; controlo de fronteiras externas e migração irregular). Esta área é uma competência partilhada entre a UE e os Estados-membros[7] e com um raio de ação territorial mais alargado, ou seja, de dimensão interna e externa.

Enquanto, a segurança pública tem um âmbito mais restrito e local. Refere-se à manutenção da ordem pública dentro dos Estados; por ex., a determinada criminalidade menos grave (ex. furto, vandalismo), manifestações violentas, segurança rodoviária. Sendo uma competência nacional, mas pode justificar restrições a certos direitos da UE, como a livre circulação, desde que sejam proporcionais e justificadas[8].

A jurisprudência do TJUE mostra que o conceito de segurança interna na UE deve ser equilibrado com os direitos fundamentais e os princípios do direito da União. Embora os Estados-membros tenham autonomia para definir ameaças à sua segurança nacional, as medidas de segurança interna devem ser proporcionais, justificadas e compatíveis com o direito da UE.

---

6 Caso *La Quadrature du Net* (C-511/18, C-512/18 e C-520/18), p. 99.
7 Caso J. N. (C-601/15 PPU); Caso *Digital Rights Ireland* (C-293/12) e *La Quadrature du Net* (C-511/18, C-512/18 e C-520/18), *Tjebbes* (C-221/17).
8 Caso *Tsakouridis* (C-145/09).

O TJUE procura distinguir ambas as conceções pela sua natureza, gravidade e o caráter específico das circunstâncias que o constituem e do risco geral, de cada caso concreto. Nem sempre ficou claro quando uma ameaça à segurança pública se torna uma ameaça à segurança nacional, e, o Tribunal também não definiu o que constitui um risco sério à segurança pública (Mitsilegas, 2024, p. 1456).

A ordem pública e a segurança pública têm sido tradicionalmente analisadas como derrogações ao direito da União e, portanto, como manifestação de um poder residual dos Estados-membros para protegerem as "suas" conceções (nacionais) de ordem e segurança pública e a sua capacidade de fornecer estes bens públicos (Coutts, 2024, p. 1484). No entanto, o direito da UE, incluindo, o artigo 72.º e o artigo 4.º (2), inclusive, não constitui uma derrogação do direito da UE, nem uma cláusula de emergência suscetível de justificar desvios ao quadro constitucional, pelo que não deve ser interpretada de forma restritiva, mas como uma medida de flexibilidade excecional incorporada no quadro constitucional da UE (Thym, 2021, pp. 1408-1409; *Editorial comments*, 2024, p. 290).

4. CONCLUSÕES: DE UMA ÁREA EM CONSTRUÇÃO

O termo de segurança interna surgiu primeiro no quotidiano dos Estados e da sociedade, em geral por oposição e necessidade, de distinguir a polícia das: atividades de justiça; das ações de guerra (segurança externa); das polícias de regimes autoritários. Ou seja, um conceito construído ou distinguido, em parte, pela negativa e por necessidade pragmática.

Por outro lado, a emergência da segurança interna da UE conduziu e contribuiu para uma aproximação e confusão, com uma conceção tradicional de segurança nacional. Sendo que, no caso português o sistema de segurança interna, também por influência da UE é atualmente o modelo mais próximo de uma versão integrada de Segurança Nacional, ainda amputado, de uma articulação e coordenação ao nível da formação e de uma estratégia, ou seja, a componente formativa e preditiva da segurança interna.

Em síntese, apesar da segurança interna ganhar relevância no debate público, pela via de acontecimentos marcantes que foram suscetíveis de gerar insegurança, associado ao discurso político consequente trouxeram para a ordem do dia algumas matérias de segurança interna, desde logo a discussão da sua natureza e dos limites teóricos, territoriais, materiais e funcionais. Contudo, a agenda da academia não acompanhou o estudo holístico da segurança interna,

dado que ficou centrada no impacto de determinados acontecimentos marcantes (ex. terrorismo, migrações) e, por vezes, na desconexão entre os factos e a realidade, o que justifica, cada vez mais, a necessidade do seu estudo e um quadro teórico coerente, por necessidade analítica intrínseca, mas também porque a realidade de segurança interna foi transformada, pelo que existe, igualmente, uma necessidade prática, desde logo no campo da formação e de investigação.

REFERÊNCIAS BIBLIOGRÁFICAS

Berthelet, P., 2016. *La sécurité intérieure européenne: aspects normatifs d'une politique publique*. Thèse de Doctorat en Droit Public. Université de Pau et des Pays de L'adour.

Bossong, R., & Rhinard, M., 2012. European internal security as a public good. *European Security, 22*(2), 129–147.

Brandão, A. P., 2016. European Union Security Actorness: The Comprehensive Approach Hampered by Policy Differentiation. *Nação e Defesa*, 144, 103-131.

Brandão, A. P., 2022. União Europeia e Segurança Interna Coletiva: Progressos e Tensões Dilemáticas de um Ator em Construção». In Maria J. F. Monte, Flávia N. Loureiro e Pedro J. Morais (ed.). *Prevenção, Policiamento e Segurança - Implicações nos Direitos Humanos. I Congresso Internacional JusCrim*, Universidade do Minho, 141-158.

Brouillet, P., 2013. Sécurité intérieure et gestion de la violence. In: F. Debove, et O. Renaudie, (coords.). *Sécurité intérieure. Les nouveaux défis*. Vuibert, 3-10.

Brouillet, P., 2023. *La sécurité intérieure: un concept creux? Conferência no Musée de la Gendarmerie*, Melun, 30 de março de 2023. https://www.force-publique.net/2023/03/24/a-vos-agendas-jeudi-30-mars-2023/

Chetrit, T., 2012. *Sécurité intérieure et criminalité contemporaine en France*. Thèse de Doctorat en Droit Public. Université Panthéon - Assas - Paris II.

Comiskey, J., 2018. Theory for Homeland Security. *Journal of Homeland Security Education*, 7, 29-45.

Coste, F., 2011. *L'adoption du concept de sécurité nationale: une révolution conceptuelle qui peine à s'exprimer*. Recherches & Documents N° 03. Fondation pour la Recherche Stratégique. https://archives.frstrategie.org/publications/recherches-et-documents/l-adoption-du-concept-de-securite-nationale-une-revolution-conceptuelle-qui-peine-a-s-exprimer-03-2011

Coste, F., 2011. Défense globale, sécurité intérieure, sécurité nationale : quelle distinction ? Quelles articulations?», *Cahiers français*, n°360, 36-40.

Coutts, S., 2024. The Evolution of Public Order and Public Policy in EU Law. *European Papers*, 9 (3), pp. 1475-1485.

Crawford, A., (2014). L'hétérogénéité du concept de sécurité: ses implications sur les politiques publiques, la justice et la durabilité des pratiques. *Cahiers de la securite et de la justic*e, 27/28, 25-34.

Dahl, E. and Ramsay, J., 2024. Should Homeland Security Studies Survive? *Journal of Homeland Security and Emergency Managemen*t, 21 (1), 1–26.

Debove, F. et Renaudie, O. (dir.), 2013. Sécurité intérieure. *Les nouveaux défis*. Vuibert.

Debove, F. et Renaudie, O. Avant-propos. 2013. In: F. Debove et O. Renaudie (dir.). *Sécurité intérieure. Les nouveaux défis*. Vuibert, XI-XIII.

Doaré, R. and Frustié, M., 2019. *Droit de la sécurité intérieure*. Gualino.

Dupin, B., 2023. *La sécurité intérieure de l'UE: approche juridique d'une construction politique*. Thèse de Doctorat en Droit Public. Université de Pau et des Pays de L'adour.

Editorial Comments, 2024. The passion for security in European societies. *Common Market Law Review*, 61, 283-296.

Eriksson, J. and Rhinard, M., 2009. The internal–external security nexus: notes on an emerging research agenda. *Cooperation and Conflict*, 44 (3), 243–267.

Falkow, M., 2013. *Does Homeland Security Constitute an Emerging Academic Discipline?*. Master's Thesis. Naval Postgraduate School Monterey.

Fernandes, A. H., 2011. *Acolher ou Vencer? A Guerra e a Estratégia na Atualidade*. Esfera do Caos.

Gonçalves, G., 2012. Polícia, ordem pública e "novas" formas de vigilância: as dinâmicas e os dilemas da segurança. *Análise Social*, 47 (204), 713-723.

Greene, S. (2022). The limits of exporting the homeland security construct: lessons from the Gulf. *Defence Studies*, 22 (2), 231-252.

Hermenegildo, R. S., 2013. Autonomização, Emergência e Afirmação da Segurança Interna da União Europeia. *Nação e Defesa*, 135, 153-171.

Hermenegildo, R. S., 2016. "Segurança Interna Europeia em perspetiva. Abordagem teórico-concetual e desafios prementes", *Revista Direito e Segurança*, 7, 179-216.

Hermenegildo, R. S., 2017. Uma Matriz Teórica da "Segurança Interna" da União Europeia, *Nação e Defesa*, 146, pp. 106-133.

Hermenegildo, R. S., 2018. A "Segurança Interna" da União Europeia: o caso da Guarda Costeira e de Fronteiras. *Proelium*, VII (14), 147-182.

Hermenegildo, R. S., 2024. Implicações da Guerra da Ucrânia na segurança da União Europeia: incremento da supranacionalização? *Relações Internacionais*, 83, 29-42.

Heyeghe, H., 2018. L'avènement de la coproduction de la sécurité: le bilan et les acteurs, *Les Annales de droit*. 12. Disponível em http://journals.openedition.org/add/978; DOI: https://doi.org/10.4000/add.978

Icard, V., Lemaire, É. et Maillard, J., 2024. Les recompositions du gouvernement de la sécurité. *Revue française d'administration publique*, 185(1), 7–23.

Kiltz, L. and Ramsay, J., 2012. Perceptual Framing of Homeland Security. *Homeland Security Affairs*, 8 (15), 1-26.

Leyen, V., 2024. *Europe's Choice – Political Guidelines for the next European Commission 2024-2029*, Alocução no Parlamento Europeu, Estrasburgo, 18 de julho. https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf

Lourenço, N., (coord), 2006. *Estudo para a reforma do modelo de organização do sistema de segurança interna: relatório final*. Instituto Português de Relações Internacionais. Universidade Nova de Lisboa.

Maillard, J., 2010. Les politiques de sécurité. In: O. Borraz et V. Guiraudon. *Politiques publiques 2*. Presses de Sciences Po, 57–77.

Malochet V., 2021a. La sécurité est-elle vraiment "l'affaire de tous"? Les límites de la participation citoyenne en France dans un domaine typiquement régalien. *Participations, à paraître*, 29, pp. 41-71.

Malochet, V., 2021b. La pluralisation du policing en France. Logiques d'hybridation, effets de tropisme et enjeux d'articulation, *Sciences et actions sociales* [en ligne], 16. http://www.sas-revue.org/88-n-16/dossier-n-16/227-la-pluralisation-du-policing-en-france. Consultada em 14/05/2025

Malochet, V., (2023). La pluralisation du policing local. In: J. Maillard et W. Skogan. *Police et société en France*. Presses de Science Po. 161-180.

Malochet, V., (2024). Les gendarmes et le partenariat local sous l'ère de la PSQ: enjeux d'ancrage et *continuum* de sécurité dans les zones rurales et périurbaines. *Revue française d'administration publique*, 1, 155-173.

Malochet, V. et Ocqueteau, F., 2020. Gouverner la sécurité publique Le modèle français face à la pluralisation du policing. *Gouvernement et action publique*, 9 (1), 9-31.

Melchior, P., 1999. La construction d'une nouvelle doctrine de sécurité. *Revue française d'administration publique*, 91, 387-398.

Mitsilegas, V., 2024. Reconceptualising Security in the Law of the European Union. *European Papers*, 9 (3), 1438-1473.

Morag, N., 2011. Comparative Homeland Security: *Global Lessons*. Wileyp.

Mulle, C., 2024. European Public Policy and Restriction of Free Movement of Persons in EU Law. *European Papers*, 9 (3), 1408-1423.

Palo, L., 2021. *L'évaluation de la sécurité intérieure par le législateur*. Master en Droit. Aix-Marseille Université Faculté de Droit et de Science Politique.

Places, S. B., 2024. Introduction: Public order and public security in EU law. Time for Reappraisal. *European Papers*, 9 (3), 1316-1328.

Pelfrey, P. and Kelley, W., 2013. Homeland Security Education: A Way Forward. *Homeland Security Affairs*, 9 (3), 1-12.

Renaudie, O., 2018. Les mutations de la sécurité intérieure: l'État transformé?. *Civitas Europa*, 40, 53-66.

Roché, S., 2004. Vers la démonopolisation des fonctions régaliennes: Contractualisation, territorialisation et européanisation de la sécurité intérieure. *Revue française de science politique*, 54 (1), 43–70.

Smith, S. and Acharya, A., 2002. The Concept of Security Before and After September 11. *Institute of Defence and Strategic Studies*, Working Paper, 23. https://www.rsis.edu.sg/rsis-publication/idss/23-wp023-the-concept-of-securit/

Teixeira, N. S., (coord), 2006. *Estudo para a reforma do modelo de organização do sistema de segurança interna: relatório preliminar*. Lisboa: Instituto Português de Relações Internacionais. Universidade Nova de Lisboa.

Thourot A. et Fauvergue J., 2018. *D'un continuum de sécurité vers une sécurité globale. Rapport de la mission parlementaire*. https://www.vie-publique.fr/rapport/37622-dun-continuum-de-securite-vers-une-securite-globale

Thym, D., 2021. Article 72 [Clause on Maintaining Internal Security by Member States]. In: H.-J. Blanke, S. Mangiameli (eds.). *Treaty on the Functioning of the European Union – A Commentary*. Springer.

Trauner, F., 2013. *The internal–external security nexus: more coherence under Lisbon?*. EUISS – Occasional Paper, 89.

Turmo, A., 2022. National security as an exception to EU data protection standards: The judgment of the Conseil d'État in French Data Network. *Common Market Law Review*, 59, 203-222.

Verdelhan, H., 2024. Art. 72 TFEU as Seen by the Court of Justice of the EU: Reminder, Exception, or Derogation?. *European Papers*, 9 (3), 1330-1364.

White, R., 2018. A Theory of Homeland Security. *Journal of Homeland Security and Emergency Management,* 15 (1), 3-21.

ESTUDO 2 – FRONTEX E A SOBERANIA NACIONAL: DESAFIOS E IMPLICAÇÕES PARA OS ESTADOS-MEMBROS DA UNIÃO EUROPEIA

FRONTEX AND NATIONAL SOVEREIGNTY: CHALLENGES AND IMPLICATIONS FOR THE MEMBER STATES OF THE EUROPEAN UNION

Cátia Sofia Correia Tomás
Capitão GNR

RESUMO

A Agência Europeia da Guarda de Fronteiras e Costeira (Frontex) assume um papel central na gestão das fronteiras externas da União Europeia (UE), especialmente após a crise migratória de 2015. Este estudo investiga de que modo as operações da Frontex influenciam a soberania nacional dos Estados-Membros, com enfoque no Mar Egeu e no período pós-2015. Analisa-se a tensão entre integração europeia e autonomia nacional, respondendo à questão: "De que forma as operações da Frontex impactam a soberania nacional dos Estados-Membros da UE na gestão das suas fronteiras?".

A metodologia qualitativa adotada baseou-se na análise de fontes primárias e secundárias e em estudos de caso (Operação *Poseidon* e cooperação Frontex-Marrocos). Os resultados evidenciam um impacto significativo e multifacetado sobre a soberania nacional, destacando-se a transferência progressiva de competências operacionais para uma entidade supranacional, consagrada nos Regulamentos (UE) 2016/1624 e 2019/1896, que estabelecem um corpo permanente de guardas de fronteira e promovem a centralização tecnológica e operacional. Esta dinâmica gera tensões estruturais, evidenciadas pela resistência de alguns Estados-Membros aos mecanismos de partilha de responsabilidades migratórias e pelas assimetrias na implementação das políticas europeias.

O estudo demonstra que a soberania nacional é reconfigurada, emergindo um paradigma de soberania partilhada, em que o controlo formal permanece nos Estados-Membros, mas o exercício prático decorre num quadro de interdependência europeia. Adicionalmente, a crescente securitização da migração e a externalização do controlo fronteiriço, através da cooperação com países terceiros, levantam preocupações quanto ao respeito pelos direitos humanos e à autonomia na formulação de políticas migratórias.

Conclui-se que a atuação da Frontex, embora reforce a segurança coletiva da UE, impõe limitações à autonomia estatal, num processo dinâmico que exige ponderação entre

segurança, soberania e direitos fundamentais. A Frontex constitui, assim, um exemplo paradigmático da evolução da soberania no século XXI, caracterizada por governação multinível.

Palavras-chave: Frontex, Soberania Nacional, União Europeia, Gestão de Fronteiras, Segurança, Migração

ABSTRACT

The European Border and Coast Guard Agency (Frontex) plays a central role in managing the external borders of the European Union (EU), particularly following the 2015 migration crisis. This study investigates how Frontex operations influence the national sovereignty of Member States, with a focus on the Aegean Sea and the post-2015 period. The analysis addresses the tension between European integration and national autonomy, answering the research question: "In what ways do Frontex operations impact the national sovereignty of EU Member States in border management?"

A qualitative methodology was adopted, based on the analysis of primary and secondary sources and case studies (such as Operation Poseidon and Frontex-Morocco cooperation). The findings reveal a significant and multifaceted impact on national sovereignty, notably through the progressive transfer of operational competences to a supranational entity, as enshrined in Regulations (EU) 2016/1624 and 2019/1896, which establish a permanent border guard corps and promote technological and operational centralisation. This dynamic generates structural tensions, evidenced by the resistance of some Member States to responsibility-sharing mechanisms and by asymmetries in the implementation of European policies.

The study demonstrates that national sovereignty is being reconfigured, giving rise to a paradigm of shared sovereignty, in which formal control remains with Member States, but practical exercise occurs within a framework of European interdependence. Additionally, the increasing securitisation of migration and the externalisation of border control, through cooperation with third countries, raise concerns regarding respect for human rights and autonomy in migration policy formulation.

It is concluded that, while Frontex's actions strengthen the EU's collective security, they impose limitations on state autonomy, in a dynamic process that requires constant balancing between security, sovereignty, and fundamental rights. Frontex thus constitutes a paradigmatic example of the evolution of sovereignty in the 21st century, characterised by multi-level governance.

***Keywords**: Frontex, National Sovereignty, European Union, Border Management, Security, Migration*

1. INTRODUÇÃO

A Agência Europeia da Guarda de Fronteiras e Costeira (Frontex), desempenha um papel importante na gestão das fronteiras externas da União Europeia (UE). Este estudo analisa o impacto das operações da Frontex na soberania nacional dos Estados-Membros da União Europeia (UE), enfatizando os desafios e implicações decorrentes desta relação.

O objeto deste estudo centra-se na interação entre as atividades da Frontex e a autonomia dos Estados-Membros na gestão das suas fronteiras. A investigação delimita-se temporalmente ao período pós-2015, marcado pela crise migratória europeia, e geograficamente às fronteiras externas da UE, com especial atenção para o Mar Egeu.

Os objetivos principais desta investigação são: analisar o impacto das operações da Frontex na soberania nacional dos Estados-Membros; identificar as tensões entre a integração europeia e a autonomia nacional na gestão de fronteiras; e avaliar os desafios e perspetivas futuras para o equilíbrio entre segurança e soberania.

A questão central de investigação é: "De que forma as operações da Frontex impactam a soberania nacional dos Estados-Membros da UE na gestão das suas fronteiras?".

A metodologia adotada baseia-se numa análise qualitativa de fontes primárias e secundárias, complementada por estudos de caso específicos, visando oferecer uma compreensão aprofundada das complexidades inerentes à relação entre as operações da Frontex e a soberania dos Estados-Membros da UE.

2. A FRONTEX E O SEU PAPEL NA UNIÃO EUROPEIA

2.1. Origem e evolução da Frontex

A Agência Europeia da Guarda de Fronteiras e Costeira (Frontex), foi criada em 2004 enquanto resposta à crescente necessidade de uma abordagem comum para o controlo das fronteiras externas da União Europeia. A fundação da Agência surgiu num contexto de aumento dos fluxos migratórios e da criminalidade transfronteiriça, que exigiam uma vigilância mais eficaz para garantir a segurança interna dos Estados-Membros. O Acordo de Schengen[9], que estabelece um espaço

[9] Acordo de Schengen, de 14 de junho de 1985, entre os Governos dos Estados da União Económica Benelux, da República Federal da Alemanha e da República Francesa relativamente à eliminação gradual de controlos nas fronteiras comuns.

sem fronteiras internas dentro da UE, veio impor a necessidade de controlar as fronteiras externas levando à criação da Frontex enquanto mecanismo de cooperação entre os países da UE (Frontex, 2020). Desde a sua fundação, a Frontex passou por várias mudanças significativas. Em 2016, em resposta à crise migratória que afetou a Europa, a agência foi reestruturada e teve o seu mandato ampliado. O Regulamento (UE) 2016/1624 conferiu à Frontex novos poderes, permitindo-lhe coordenar operações conjuntas entre os Estados-Membros, mas também realizar ações operacionais com recursos próprios. A evolução da Frontex continuou com o Regulamento (UE) 2019/1896, que veio estabelecer um corpo permanente de guardas de fronteira. Este regulamento contempla um aumento significativo no número total de agentes da Frontex, para 10.000 até 2027, revelando uma mudança na abordagem da migração e da segurança na Europa. Em julho de 2024 a presidente da Comissão Europeia, Ursula von der Leyen, discutiu no Parlamento Europeu o aumento da segurança nas fronteiras externas da Europa com o apoio da Frontex, informando que poderia aumentar para 30.000 o número de agentes (Parlamento Europeu, 2024). Esta alteração, demonstra a transição de uma postura predominantemente humanitária para uma perspetiva mais voltada para a segurança nacional (Carrera et al., 2019).

O mandato da Frontex abrange várias competências de gestão das fronteiras externas da UE. A agência implementa e coordena operações conjuntas nos Estados-Membros para reforçar o controlo das fronteiras, as quais envolvem a projeção de meios humanos e de equipamento em áreas críticas, com o objetivo de prevenir a imigração ilegal e combater a criminalidade transfronteiriça (Frontex, 2020). Ademais, a Frontex realiza análises sobre as ameaças à segurança nas fronteiras externas, permitindo que os Estados-Membros ajustem as suas políticas em função da informação obtida. A agência Frontex, fornece ainda formação às autoridades nacionais em diversas matérias que envolvem o controlo de fronteiras e proporciona apoio técnico e logístico, através do desenvolvimento de treino e formação padronizados e da partilha de boas práticas entre os Estados-Membros (Comissão Europeia, 2021). A capacidade de adquirir equipamentos, como navios e drones, também veio permitir uma resposta mais rápida e eficaz às situações de crise nas fronteiras externas da UE. A utilização destas tecnologias integra a estratégia da Frontex para melhorar a vigilância das fronteiras e para aumentar a eficiência das operações (Bigo et al., 2019).

2.2. Coordenação das Políticas de Segurança e de Controlo da Imigração

A Frontex assume um papel central na coordenação das políticas de segurança e controlo da imigração na UE. A atuação da agência está interligada aos principais acordos que moldam a política migratória europeia, como os Acordos de Schengen e a Convenção de Dublin. O Acordo de Schengen estabelece um espaço sem fronteiras internas na UE, exigindo o controlo das fronteiras externas para garantir a segurança interna dos Estados-Membros (União Europeia, s.d.). Por sua vez, a Convenção de Dublin regula as condições sob as quais os pedidos de asilo são processados na UE, colocando as responsabilidades nos Estados-Membros onde os migrantes chegam primeiro. A Frontex auxilia na implementação deste acordo através das operações de controlo fronteiriço (Conselho Europeu, 2021), e contribui para a implementação do Novo Pacto Europeu sobre Migração, designado por Pacto das Migrações e Asilo[10], proposto em 2020 e aprovado pelo Parlamento Europeu em abril de 2024 e pelo Conselho em maio de 2024, que visa intensificar o controlo das chegadas irregulares à UE e acelerar os processos de retorno dos migrantes ilegais.

O Pacto das Migrações e Asilo visa criar um sistema de migração e asilo mais justo, eficiente e sustentável na União Europeia, com o objetivo de melhorar a gestão dos fluxos migratórios e reforçar a solidariedade entre os Estados-Membros. Para alcançar este objetivo, o Pacto propõe um conjunto de medidas chave, incluindo um procedimento de triagem na fronteira para identificar rapidamente quem precisa de proteção, um mecanismo de solidariedade obrigatória para partilhar a responsabilidade entre os Estados-Membros, o reforço da cooperação com países terceiros para gerir os fluxos migratórios e combater as causas da migração, e a revisão do Regulamento de Dublin para determinar o Estado-Membro responsável pela análise de um pedido de asilo.

Por outro lado, a atuação da Frontex tem sido alvo de críticas devido à crescente tecnologização e securitização do controlo das fronteiras. Oliveira Martins e Gabrielsen Jumbert (2022) analisam de que forma as recentes dinâmicas

[10] O Novo Pacto Europeu sobre Migração e Asilo, também conhecido como Pacto sobre Migração e Asilo, é um conjunto de propostas legislativas apresentado pela Comissão Europeia em setembro de 2020 com o objetivo de reformar as políticas de migração e asilo da União Europeia (UE), (Comissão Europeia, 2020).

dos fluxos migratórios intensificaram a dependência de tecnologias emergentes na gestão das fronteiras da UE. Os autores destacam o uso crescente de Veículos Aéreos Não Tripulados (UAV)[11], comummente conhecidos como drones, equipados com tecnologias específicas de informação e de vigilância, que têm sido cada vez mais entendidos como fundamentais na gestão da migração na UE. Esta tendência reflete uma abordagem que carateriza os migrantes tanto como potenciais ameaças à segurança quanto como indivíduos que necessitam de resgate e de proteção. O referido enquadramento desencadeia novas dinâmicas de securitização que retratam a questão migratória como passível de ser gerida através da utilização de tecnologia de ponta. Nesta lógica, os problemas e as soluções de segurança são coproduzidos dentro de uma complexa rede multicamada de atores públicos e privados (Oliveira Martins & Gabrielsen Jumbert, 2022). Esta abordagem suscita novas reflexões sobre o equilíbrio entre segurança, direitos humanos e a soberania dos Estados-Membros na gestão das fronteiras da UE.

2.3. Gestão Europeia Integrada das Fronteiras

A gestão europeia integrada das fronteiras, enquanto conceito, orienta as atividades da Frontex dentro do contexto mais amplo da política migratória da UE. Este modelo visa fortalecer o controlo nas fronteiras externas, mas também promover uma abordagem coesa entre os Estados-Membros na gestão dos fluxos migratórios, integrando as políticas nacionais com as europeias para enfrentar desafios comuns relacionados com a segurança e com a imigração.

A Frontex sincroniza a gestão integrada das fronteiras, apoiando os Estados-Membros, nomeadamente através da coordenação de operações conjuntas e de assistência na implementação de normas comuns em matéria de vigilância e de controlo das fronteiras (Frontex, 2020). A gestão integrada das fronteiras também implica uma estreita cooperação com os países terceiros, por forma a abordar as causas subjacentes à migração irregular. Através da implementação de parcerias com os países terceiros, a Frontex promove ações conjuntas que visam melhorar as condições locais e reduzir os incentivos à migração irregular (Carrera et al., 2019).

Contudo, as diferenças nas políticas nacionais relativamente à imigração, dificultam uma resposta comum perante os desafios enfrentados pela UE,

[11] Unmanned Aerial Vehicles (UAV) ou Veículos Aéreos Não Tripulados (VANT).

existindo preocupações entre o equilíbrio das necessidades de segurança e os direitos humanos dos migrantes durante as operações conduzidas pela Frontex (Bigo et al., 2019).

3. SOBERANIA NACIONAL NO CONTEXTO DA GESTÃO DE FRONTEIRAS DA UE

3.1. Aplicabilidade e Tensões na Gestão de Fronteiras

O conceito de soberania nacional, tradicionalmente entendido como a autoridade suprema de um Estado sobre seu território e população, não é consensual no contexto da UE.

A integração europeia, com a transferência de competências para instituições supranacionais, levanta questões sobre a soberania nacional, especialmente na gestão de fronteiras. A visão clássica da soberania enquanto "poder supremo na ordem interna e poder autónomo e independente na ordem internacional" (Moreira, 2014) é desafiada pela integração europeia. Autores como Nuno Severiano Teixeira (2017) e António de Sousa Lara (2015) complementam essa visão, destacando a capacidade do Estado de exercer autoridade e se relacionar com outros em pé de igualdade, e a indivisibilidade da soberania.

No contexto da UE, o conceito de soberania tem vindo a evoluir com a transferência de competências para instituições supranacionais. Jean Bodin, no século XVI, definiu soberania como "poder absoluto e perpétuo", mas Hermenegildo (2006a) argumenta que essa visão clássica perde força na integração europeia. Krasner (1999) identifica quatro tipos de soberania, sendo a legal internacional e a vestefaliana particularmente relevantes na UE, onde os Estados-Membros delegam poderes em instituições supranacionais. A soberania moderna é assim compreendida como uma soberania partilhada, através da cooperação dos Estados de modo a enfrentar desafios comuns (Keohane, 2002). Moravcsik (1998) defende que os Estados cedem voluntariamente parte da sua soberania para alcançar objetivos comuns. Por sua vez, Hermenegildo (2006b) destaca a transferência de competências soberanas para modelos cooperativos, participados e hierarquizados, desafiando assim as noções clássicas de soberania.

A integração europeia gera assim tensões entre soberania nacional e a necessidade de cooperação. Schimmelfennig e Sedelmeier (2020) salientam a constante negociação entre os benefícios da integração e a preservação da autonomia nacional.

O princípio da subsidiariedade visa equilibrar essas tensões, mas a sua interpretação prática é controversa, sobretudo em aspetos de segurança e de imigração (Schütze, 2009).

Börzel (2005) identifica diferentes padrões de "europeização" entre os Estados-Membros, com alguns mais recetivos à integração e outros mais resistentes à transferência de competências, como é verificado no contexto da gestão fronteiriça. Esta dinâmica é particularmente visível em países como a Hungria e a Polónia, os quais têm frequentemente entrado em conflito com as políticas da União Europeia (Scipioni, 2018). A jurisprudência do Tribunal Constitucional Federal da Alemanha (TCF) tem sido um exemplo dessa tensão, reiterando que, embora a Alemanha tenha transferido competências para a UE, tal não deve comprometer a sua soberania nacional (Wohlfahrt, 2009). Esta posição reflete uma resistência à ideia de que a integração europeia deva ocorrer em detrimento da autonomia nacional.

O princípio do primado do direito da UE sobre o direito nacional, pode gerar conflitos significativos, especialmente quando as normas europeias colidem com as constituições nacionais (Hix & Hoyland, 2011). Embora o direito da UE prevaleça sobre o direito nacional, a sua aplicação não é isenta de limites e desafios, exigindo uma análise cuidadosa e uma ponderação de interesses em cada caso concreto. Esta situação é particularmente relevante na gestão fronteiriça, em que as políticas nacionais podem ser desafiadas pelos regulamentos europeus que visam uma abordagem mais coesa e integrada. A soberania nacional no contexto da UE evolui assim para um modelo de soberania partilhada, com desafios e tensões constantes.

3.2. O Espaço Schengen e as suas implicações

O Espaço Schengen, exemplo tangível da integração europeia, tem implicações significativas para a soberania nacional. Zaiotti (2011) defende que o Espaço Schengen transformou o conceito de fronteiras na Europa, através da criação da distinção entre fronteiras internas e externas da UE. Estabelecido para permitir a livre circulação de pessoas entre os diversos Estados-Membros que o integram, o Espaço Schengen implica que os países abdiquem do controlo total sobre as suas fronteiras internas em prol de um controlo mais rigoroso das fronteiras externas (União Europeia, s.d). Esta cedência de soberania é compensada pela premissa de uma segurança coletiva: todos os membros do Espaço Schengen comprometem-se a manter padrões comuns para o controlo das fronteiras externas. As implicações do Espaço Schengen são, contudo, complexas. Por um lado, o acordo facilita a livre

circulação de pessoas e bens no seio da UE, promovendo a integração económica e social. Mas por outro lado, alguns eventos, como por exemplo os ataques terroristas ou as crises migratórias, podem levar à reintrodução temporária de controlos nas fronteiras internas pelos Estados-Membros, suscitando questões sobre a eficácia e resiliência do sistema Schengen (Comissão Europeia, 2021). Tsoukala (2005) analisou de que forma a implementação do Espaço Schengen alterou a vigilância e controlo, levando a uma securitização da migração. Esta mudança teve impactos profundos nas políticas nacionais de segurança e na perceção pública da imigração. O funcionamento do Espaço Schengen depende da cooperação entre os Estados-Membros na gestão das fronteiras externas. Neste contexto, a Frontex atua através da coordenação de operações conjuntas e do apoio técnico aos países que enfrentam maiores desafios na vigilância das fronteiras (Frontex, 2020). Contudo, esta interdependência expõe vulnerabilidades; se um Estado não cumprir com as suas obrigações relativamente ao controlo das fronteiras externas, tal pode comprometer a segurança de todo o Espaço Schengen. A crise migratória de 2015 evidenciou as fragilidades do Acordo de Schengen, levando à reintrodução de controlos fronteiriços internos. O fluxo migratório sem precedentes exerceu pressão sobre os sistemas de asilo e acolhimento, especialmente na Grécia e Itália. De acordo com Niemann e Zaun (2018), esta crise desafiou o princípio de solidariedade entre os Estados-Membros, com alguns Estados a implementarem controlos unilaterais.

O Código das Fronteiras Schengen[12] permite que os Estados-Membros reintroduzam temporariamente o controlo nas fronteiras internas em circunstâncias excecionais, nomeadamente em caso de ameaça grave à ordem pública ou à segurança interna. A título ilustrativo, desde 2022 a Alemanha reintroduziu 15 controlos, perfazendo um total de 1348 dias, na fronteira com a Polónia, Suíça e República Checa, em resposta aos fluxos de migração irregular e contrabando de migrantes (Comissão Europeia, 2025). De igual modo, a Bulgária implementou controlos na fronteira com a Roménia em virtude de riscos de segurança relacionados com a migração ilegal. Importa sublinhar que a reintrodução do controlo fronteiriço consubstancia uma medida excecional e temporária, sujeita aos princípios da necessidade e da proporcionalidade, com duração limitada e âmbito restrito ao estritamente necessário para fazer face à ameaça identificada.

[12] Regulamento (UE) 2016/399 do Parlamento Europeu e do Conselho, de 9 de março de 2016.

Tabela 1 – Controlo Fronteiriço em Estados-Membros (2022-2025)

País	*Ano*	*Nº de Controlos*	*N.º Total de Dias*
Alemanha	2022	**2**	**233**
	2023	**5**	**288**
	2024	**7**	**643**
	2025	**1**	**184**
Bulgária	2022	-	-
	2023	-	-
	2024	-	-
	2025	**1**	**181**

Fonte: Comissão Europeia (2025)

A Figura 1 apresenta um resumo dos controlos fronteiriços implementados pela Alemanha e Bulgária entre 2022 e 2025. Os dados demonstram que a Alemanha teve vários períodos de controlo ao longo destes anos, enquanto a Bulgária apenas reintroduziu o controlo em 2025[13].

3.3. Competências dos Estados-Membros na Gestão de Fronteiras

Não obstante a crescente integração europeia, os Estados-Membros preservam competências na gestão das fronteiras. Geddes e Scholten (2016) salientam que as políticas nacionais de imigração mantêm uma heterogeneidade entre os países da UE, refletindo os diferentes contextos históricos, geográficos e políticos.

No âmbito do quadro jurídico da UE, cada Estado-Membro conserva a prerrogativa de determinar as suas políticas de imigração e de controlo das fronteiras internas. Consequentemente, as decisões relativas à entrada e permanência no território nacional permanecem sob a alçada das autoridades nacionais (Carrera et al., 2019). Os Estados-Membros dispõem igualmente de autonomia para implementar medidas adicionais de segurança fronteiriça, tais como o reforço do efetivo de agentes ou o investimento em tecnologias de vigilância (Bigo et al., 2019). Esta autonomia é, contudo, contrabalançada com as exigências da legislação

[13] Os dias de controlos que se estenderam para o ano seguinte foram contabilizados apenas no ano em que se iniciaram.

europeia e pelas expectativas dos demais Estados-Membros no âmbito do sistema Schengen. Lavenex (2006) analisa o conceito de "governança externa" da UE, no qual as políticas de fronteiras e migração são progressivamente negociadas com os países terceiros. Esta abordagem tem implicações na soberania dos Estados-Membros, que devem conciliar os interesses nacionais com os objetivos coletivos da UE. Trauner e Wolff (2014) analisam como a externalização do controlo fronteiriço, através de acordos com os países vizinhos, tem reconfigurado o papel tradicional dos Estados-Membros na gestão das fronteiras. Esta tendência suscita questões sobre a responsabilidade e a prestação de contas em matéria de direitos humanos e de proteção de refugiados.

As competências dos Estados-Membros são, assim, moldadas pelos compromissos internacionais e pela necessidade de colaboração transfronteiriça para enfrentar os desafios comuns relacionados com a migração irregular e a segurança. A gestão conjunta das fronteiras externas exige uma abordagem coordenada que harmoniza as necessidades nacionais com os objetivos coletivos da UE (Comissão Europeia, 2021).

4. IMPACTO DAS OPERAÇÕES DA FRONTEX NA SOBERANIA NACIONAL

4.1. Controlo das Fronteiras e Políticas Migratórias

As operações da Frontex têm implicações no controlo das fronteiras e nas políticas migratórias dos Estados-Membros da União Europeia. A atuação da Frontex é importante para a gestão integrada das fronteiras externas da UE, num contexto de crescente securitização da migração (Frontex, 2020). Desde a sua criação em 2004, a Frontex evoluiu de uma agência de coordenação para uma entidade com capacidade operacional própria, que realiza operações em larga escala (Halilovic, 2024). Esta evolução tem impacto direto nas políticas migratórias nacionais, influenciando as decisões sobre imigração e controlo fronteiriço. Hermenegildo (2018) analisa a securitização do controlo das fronteiras e a externalização da segurança das fronteiras, evidenciando como a Frontex se tornou um agente central na implementação de políticas que priorizam a segurança. Fink (2017) corrobora esta perspetiva, analisando de que forma a atuação da Frontex contribui para a perceção da migração enquanto ameaça à segurança societal (ou identitária) europeia. Ferreira (2023) defende que as políticas de securitização

têm transformado as fronteiras em instrumentos de controlo, refletindo uma abordagem que pode comprometer os direitos dos migrantes.

O mandato da Frontex, que permite intervenções rápidas, pode resultar em ações que não respeitam integralmente os direitos humanos (Tribunal de Contas Europeu, 2021). A harmonização das políticas nacionais com as diretivas da Frontex pode restringir a autonomia dos Estados-Membros na formulação das políticas migratórias, suscitando questões sobre o equilíbrio entre integração europeia e soberania nacional no domínio da gestão fronteiriça. Em matéria de políticas migratórias, a harmonização das legislações nacionais é um objetivo central da Frontex, mas enfrenta desafios devido à diversidade das legislações existentes. Cada Estado-Membro possui leis e práticas de imigração próprias, refletindo os contextos históricos, sociais e políticos distintos (Carrera et al., 2019).

A pressão para alinhar as legislações nacionais com as normas europeias gera tensões entre as prioridades nacionais e os objetivos comuns da UE. Zaiotti (2011) observa que esta tensão é evidente na forma como os diferentes países interpretam e implementam as suas políticas de imigração. Alguns Estados-Membros adotam abordagens mais abertas, enquanto outros optam por medidas mais restritivas. Hermenegildo (2018) argumenta que a imposição de normas comuns pela Frontex pode limitar a autonomia legislativa dos Estados-Membros. Também Lopes (2020) reforça esta ideia, destacando que o novo regulamento da Agência exige adaptações significativas nas legislações nacionais, podendo resultar numa "europeização" das práticas de imigração. A harmonização pode, contudo, promover uma melhor atuação no controlo das fronteiras. A troca de informações e de conhecimento através da Frontex pode levar à adoção de políticas mais eficazes na gestão dos desafios migratórios. No entanto, esta interdependência também suscita questões sobre a responsabilidade dos Estados em respeitar os direitos humanos durante a implementação destas políticas (Halilovic, 2024).

4.2. Cooperação com Países Terceiros

A cooperação com países terceiros constitui uma estratégia central nas operações da Frontex para gerir os fluxos migratórios antes que os mesmos atinjam as fronteiras da UE. Esta abordagem envolve a concretização de acordos com países não europeus para externalizar o controlo das fronteiras (Carrera et al., 2019). Por exemplo, os acordos com países como a Tunísia e o Egito visam impedir que os migrantes partam em direção à Europa ou transferir o processamento

dos pedidos de asilo para fora do território europeu. Esta externalização tem implicações significativas para a soberania nacional dos Estados-Membros; ao delegar responsabilidades de controlo fronteiriço em países terceiros, os Estados podem comprometer a sua capacidade de garantir que os direitos humanos sejam respeitados nestas operações (Halilovic, 2024). Ademais, esta prática pode legitimar regimes autoritários de países terceiros, uma vez que fornecem apoio financeiro e logístico às suas Forças de Segurança.

Ferreira (2023) destaca de que forma esta cooperação pode criar condições mais precárias para os migrantes e assim causar preocupações sobre o impacto humanitário destas políticas. A detenção em massa de migrantes nos centros fora da UE tem sido criticada por organizações de direitos humanos como uma violação dos direitos fundamentais (Conselho da Europa, 2021). Por outro lado, a dependência da cooperação com países terceiros pode criar vulnerabilidades para os Estados-Membros da UE. Se os países terceiros não cumprirem as suas obrigações ou se ocorrerem mudanças políticas internas que afetem a sua capacidade de cooperar, isso pode resultar num aumento inesperado nos fluxos migratórios para a Europa (Scipioni, 2018)

5. ESTUDO DE CASO

5.1. Operação *Poseidon* no Mar Egeu (Grécia)

A Operação *Poseidon*, coordenada pela Frontex no Mar Egeu, é uma das iniciativas da agência na gestão das fronteiras externas da UE. A Operação teve o seu início em 2006, com o objetivo de combater a imigração irregular e o tráfico de seres humanos, além de reforçar o controlo fronteiriço na região. Entre 2015 e 2023, a Operação *Poseidon* resgatou mais de 200.000 migrantes no Mar Egeu, mas também resultou na detenção e devolução de milhares de pessoas para países terceiros (Frontex, 2023). Em 2023, a operação contou com cerca de 600 agentes destacados e a utilização de equipamentos tecnológicos avançados, como drones e navios patrulha, representando assim um aumento significativo em comparação com os 200 agentes projetados no início da operação em 2006 (Comissão Europeia, 2023).

Tabela 2 – Projeção de meios e migrantes resgatados na Operação *Poseidon*

Ano	*Migrantes resgatados*	*Migrantes devolvidos*	*Agentes envolvidos*	*Equipamentos utilizados*
2015	50.000	10.000	300	Navios patrulha
2020	30.000	15.000	500	Drones e helicópteros
2023	20.000	12.000	600	Drones e navios modernos

Fonte: Adaptado de Frontex (2023) e Comissão Europeia (2023)

Através da análise de Relatórios do Conselho da Europa (2023) e da Amnistia Internacional (2022) é possível verificar que são efetuadas várias alegações a práticas de *pushback* durante a operação, violando o princípio de *non-refoulement*[14]. Apesar da Operação Poseidon ser liderada pela Frontex, a sua execução depende da colaboração com as autoridades gregas. Este modelo gera tensões sobre a autonomia grega na gestão das suas fronteiras. A Operação implementada em resposta à crise migratória de 2015, desafiou os paradigmas tradicionais de gestão fronteiriça e catalisou uma resposta coordenada a nível europeu (Scipioni, 2018). Os objetivos estratégicos da operação são multifacetados, abrangendo desde a deteção prévia das embarcações suspeitas e o salvamento de vidas no mar, até à prevenção de entradas não autorizadas no espaço Schengen. Adicionalmente, a operação visa reforçar as capacidades operacionais e técnicas das autoridades gregas na gestão de fronteiras, promovendo uma abordagem que integra elementos de segurança, humanitários e de cooperação interagências. Hermenegildo (2018) argumenta que esta abordagem reflete uma tendência mais ampla na política de segurança da UE, onde a gestão de fronteiras é cada vez mais vista como um elemento integral da segurança interna e externa da União.

Os dados da Organização Internacional para as Migrações (OIM) demonstram que em 2015, antes da completa implementação da Operação *Poseidon*, cerca de 857.000 migrantes chegaram às ilhas gregas pelo Mar Egeu (OIM, 2016). Este número representava um aumento abrupto em comparação com as 41.038 chegadas registadas em 2014 (UNHCR, 2015). Após a intensificação da Operação *Poseidon* e a implementação do acordo UE-Turquia, em março de 2016, observou-se

[14] *Non-refoulement*, é o princípio de Direito Internacional segundo o qual é proibido fazer regressar ao país de origem quem procura asilo por receio de perseguição, tortura, tratamento desumano ou quaisquer outras violações de direitos humanos, em função da sua raça, religião, nacionalidade, grupo social a que pertence ou das suas opiniões políticas. Este princípio encontra-se consagrado, *inter alia*, na Convenção Relativa ao Estatuto dos Refugiados, de 1951, no seu artigo 33.º.

uma redução significativa nas chegadas. Em 2016, o número de chegadas à Grécia pelo Mar Egeu diminuiu para 173.450, uma redução de cerca de 80% em relação ao ano anterior (Frontex, 2017). Esta tendência continuou nos anos seguintes, com 29.718 chegadas em 2017 e 32.494 em 2018 (UNHCR, 2019). Comparativamente, a rota do Mediterrâneo Central, que liga a Líbia à Itália, registou 181.436 chegadas em 2016, tendo superado a rota do Egeu naquele ano (Frontex, 2017). Esta mudança nos padrões migratórios sugere um possível efeito de deslocamento, em que o reforço do controlo numa rota pode levar ao aumento do fluxo noutras.

A eficácia da Operação *Poseidon* deve ser analisada não apenas em termos de redução numérica, mas também considerando os impactos humanitários e as possíveis consequências não intencionais, como o aumento do tráfico humano ou a utilização de rotas mais perigosas pelos migrantes (Carrera et al., 2019). A presença da Frontex no Mar Egeu tem implicações profundas e multidimensionais na soberania grega. Por um lado, a operação proporciona recursos adicionais e *know-how* para o controlo das fronteiras, aliviando a pressão sobre as autoridades nacionais. Por outro, a presença de uma força multinacional em águas territoriais gregas suscita questões sobre a autonomia do Estado na gestão das suas fronteiras (Halilovic, 2024). Este cenário exemplifica o que Ferreira (2023) denomina de "soberania partilhada" ou "soberania em rede", conceitos que desafiam as noções vestefalianas tradicionais de soberania estatal. Neste contexto, a Grécia mantém formalmente o controlo sobre as suas fronteiras, mas opera num quadro de interdependência e de cooperação europeia que reconfigura o exercício prático dessa soberania. Carrera et al. (2019) argumentam que esta dinâmica reflete uma tendência mais ampla na UE, em que a integração em matéria de segurança e gestão de fronteiras está a redefinir os contornos da soberania nacional.

5.2. Cooperação Frontex-Marrocos

A cooperação entre a Frontex-Marrocos, iniciada formalmente em 2019, representa um caso paradigmático das complexas relações entre a UE e os países terceiros no âmbito da gestão de fronteiras. Do ponto de vista marroquino, como argumenta El Qadim (2022), a cooperação com a Frontex é vista como uma oportunidade estratégica para reforçar a sua posição geopolítica e obter vantagens económicas e políticas. As declarações oficiais do Ministério do Interior Marroquino destacam o papel do país enquanto "parceiro fiável" na gestão migratória, sublinhando a importância da sua contribuição para a segurança regional (Ministère

de l'Intérieur du Maroc, 2023). Contudo, têm sido expressas preocupações sobre o impacto desta colaboração nos direitos dos migrantes por organizações da sociedade civil marroquina, como a Association Marocaine des Droits Humains (AMDH). Lahlou (2023) descreve que a externalização do controlo fronteiriço da UE para Marrocos tem culminado na utilização de práticas que violam os direitos humanos, nomeadamente detenções arbitrárias e deportações forçadas.

A análise das vantagens e desvantagens desta cooperação para Marrocos revela um quadro complexo. O país beneficia de apoio financeiro e técnico significativo da UE, fortalecendo assim as suas capacidades de controlo fronteiriço (Carrera et al., 2019). Contudo, Belguendouz (2023) alega que esta cooperação compromete a soberania marroquina, transformando o país num "guarda-fronteiras" da Europa, ilustrando assim os desafios inerentes à externalização das políticas migratórias da UE. Hermenegildo (2018) argumenta que esta estratégia de externalização reflete uma tentativa da UE estender a sua influência para além das suas fronteiras formais, criando uma espécie de "fronteira avançada" que desafia as noções tradicionais de territorialidade e de soberania. Os acordos Frontex-Marrocos abrangem medidas como partilha de *intelligence* e operações conjuntas, que visam fortalecer o controlo fronteiriço e prevenir a migração irregular (Scipioni, 2018). No entanto, levantam preocupações sobre potenciais violações de direitos humanos e a externalização da responsabilidade da UE na proteção de refugiados (Conselho da Europa, 2021). Esta abordagem levanta questões éticas e legais relativamente à garantia do respeito pelos direitos humanos em operações fora do território da UE (Ferreira, 2023).

A cooperação Frontex-Marrocos origina questões complexas sobre soberania e direitos humanos na gestão de fronteiras da UE (Carrera et al., 2019). A influência da UE pode ser percecionada como uma forma de ingerência nos assuntos internos. Hermenegildo (2017) esclarece que esta situação reflete uma "soberania nacional partilhada", onde o exercício do poder soberano é moldado por forças externas e pela necessidade de colaboração. Para os Estados-Membros da UE, a dependência de países terceiros pode representar uma limitação da autonomia na gestão das fronteiras externas da União. Ferreira (2023) sugere que esta situação cria uma "soberania em rede", em que o poder decisório é distribuído entre os atores estatais e não-estatais, nacionais e supranacionais. Esta cooperação pode gerar tensões diplomáticas e dilemas éticos sobre a responsabilidade da UE na proteção dos direitos humanos fora das suas fronteiras. O Conselho da Europa

(2021) alerta para os riscos de violações de direitos humanos. Scipioni (2018) destaca a complexidade de equilibrar segurança, soberania e direitos humanos na gestão de fronteiras da UE. Num mundo caracterizado por interdependências crescentes e pelas ameaças transnacionais, a noção tradicional de soberania estatal é constantemente desafiada e reconfigurada, como é reconhecido pela Comissão Europeia (2021). Conciliar a eficácia operacional com os direitos fundamentais e a soberania exige um equilíbrio entre interesses nacionais, objetivos comunitários e as obrigações internacionais.

6. O EQUILÍBRIO ENTRE SEGURANÇA E SOBERANIA: DESAFIOS E PERSPETIVAS

O equilíbrio entre segurança e soberania representa um dos principais desafios para o futuro da Frontex e da gestão de fronteiras na UE. A crescente securitização da migração, visível na expansão das operações da Frontex, ergue preocupações sobre a erosão da soberania nacional dos Estados-Membros. Bigo et al. (2019) argumentam que a intensificação do controlo fronteiriço pode comprometer princípios fundamentais da UE, como a livre circulação de pessoas e o respeito pelos direitos humanos.

Para alcançar um equilíbrio sustentável é necessário um diálogo contínuo entre os Estados-Membros e as instituições da UE, com vista à criação de mecanismos de supervisão mais robustos para garantir que as operações da Frontex respeitem tanto as necessidades de segurança quanto a autonomia dos Estados-Membros. Ferreira da Silva (2010) destaca a importância da UE contribuir para fortalecer a soberania nacional, em vez de a fragilizar. A procura deste equilíbrio exige uma abordagem holística que conjugue as preocupações de segurança com os direitos humanos e a dignidade dos migrantes, redefinindo as políticas migratórias europeias em face das realidades contemporâneas.

As reformas propostas para a Frontex representam uma resposta estratégica às crescentes preocupações sobre supervisão operacional e respeito pelos direitos fundamentais. O Parlamento Europeu desempenha um papel importante neste processo de transformação institucional, através da proposta de medidas que visam aumentar a transparência e a responsabilização da agência. A criação do cargo de Agente de Direitos Fundamentais (Regulamento (UE) 2019/1896) e a constituição de um corpo permanente de guardas de fronteira, com a projeção de 30.000 efetivos (Parlamento Europeu, 2024), refletem a transformação em curso. Estas reformas,

a par da discussão sobre modelos de cooperação como a "soberania partilhada" em que os Estados-Membros mantêm o controlo último sobre as suas fronteiras, beneficiando simultaneamente do apoio e dos recursos disponibilizados pela Frontex (EuroDefense, 2023) e a "cooperação flexível" que permitiria aos Estados-Membros determinar o nível de envolvimento com a Frontex de acordo com as suas necessidades específicas (IPEX, 2023), procuram equilibrar as necessidades de segurança com a soberania nacional e os direitos humanos.

O sucesso destas iniciativas dependerá do diálogo, da vontade política e da capacidade de adaptação da UE e dos Estados-Membros. O desafio reside em criar um sistema suficientemente flexível para se adaptar às diferentes realidades dos Estados-Membros, mas também robusto o suficiente para enfrentar os desafios comuns à segurança.

7. CONCLUSÕES

A presente investigação permite concluir que as operações da Frontex exercem um impacto multifacetado na soberania nacional dos Estados-Membros da União Europeia, manifestando-se em quatro dimensões principais. Primeiramente, observa-se uma transferência progressiva das competências operacionais para uma entidade supranacional, consolidada pelos Regulamentos (UE) 2016/1624 e 2019/1896. Esta dinâmica é visível na coordenação de operações conjuntas, implementação de tecnologias de vigilância centralizadas e criação de um corpo permanente de guardas de fronteira. Em segundo lugar, a atuação da Frontex causa tensões estruturais entre integração e autonomia nacional, revelando divergências entre políticas nacionais e diretivas comunitárias, exemplificadas pela resistência a mecanismos de partilha de responsabilidades migratórias. A terceira dimensão envolve a redefinição do conceito de soberania, com a gestão integrada das fronteiras externas consolidando um paradigma de soberania partilhada. Por fim, observam-se assimetrias na implementação prática dos regulamentos e operações da Frontex, resultantes das disparidades geopolíticas e económicas entre os Estados-Membros.

Em resposta à questão central "De que forma as operações da Frontex impactam a soberania nacional dos Estados-Membros da UE na gestão das suas fronteiras?", conclui-se que as operações da Frontex têm um impacto significativo na soberania nacional, reforçando a segurança coletiva, mas limitando a autonomia dos Estados-Membros. Este impacto manifesta-se através

da harmonização de procedimentos, implementação de operações conjuntas e influência nas legislações nacionais.

A relação entre a Frontex e a soberania nacional configura-se como um fenómeno dinâmico, em que a integração europeia redefine constantemente os limites da autonomia estatal. As reflexões finais sugerem que o futuro da gestão das fronteiras externas da UE dependerá da conciliação entre segurança coletiva e respeito pela soberania dos Estados-Membros. Emergem aspetos críticos como o equilíbrio entre segurança e direitos humanos, a utilização estratégica da soberania nas negociações europeias, e a adaptabilidade do projeto europeu. A Frontex é um exemplo da evolução pragmática da soberania no século XXI, através da implementação de uma governação multinível que redefine as relações entre instituições nacionais e supranacionais. O sucesso deste modelo dependerá da conciliação entre eficácia operacional e responsabilização democrática.

REFERÊNCIAS BIBLIOGRÁFICAS

Amnistia Internacional. (2021). *The EU's border agency: The need for accountability*. [Relatório]

Amnistia Internacional. (2023, 17 de julho). *EU-Tunisia migration deal risks complicity in serious human rights violations*. [Comunicado de imprensa] https://www.amnesty.org/en/latest/news/2023/07/eu-tunisia-migration-deal-risks-complicity-in-serious-human-rights-violations/

Belguendouz, A. (2023). *Maroc-UE: Les enjeux de la coopération en matière de migration*. Éditions La Croisée des Chemins.

Bigo, D., Guild, E., & Ragazzi, F. (2019). *The new borders of Europe: Internal and external dimensions*. Palgrave Macmillan.

Börzel, T. A. (2005). Mind the gap! European integration between level and scope. *Journal of European Public Policy, 12*(2), 217-236.

Carrera, S., Santos Vara, J., & Strik, T. (Eds.). (2019). *Constitutionalising the external dimensions of EU migration policies in times of crisis*. Edward Elgar Publishing.

Comissão Europeia. (2021). *European Border and Coast Guard Agency (Frontex)*. https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/border-crossing/european-border-and-coast-guard-agency-frontex_en

Comissão Europeia. (2023). *Comunicação ao Parlamento Europeu e ao Conselho sobre a política estratégica plurianual para a gestão europeia integrada das*

fronteiras (COM(2023) 274 final). https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52023DC0274

Comissão Europeia. (2024). *Temporary reintroduction of border control. Migration and Home Affairs*. Comissão Europeia. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-area/temporary-reintroduction-border-control_en

Comissão Europeia. (2025). *Full list of MS notification_en.pdf*. https://home-affairs.ec.europa.eu/document/download/11934a69-6a45-4842-af94-18400fd274b7_en?filename=Full%20list%20of%20MS%20notification_en.pdf

Conselho da Europa. (2021). *A distress call for human rights: The widening gap in migrant protection in the Mediterranean. Relatório da Comissária para os Direitos Humanos*. https://rm.coe.int/a-distress-call-for-human-rights-the-widening-gap-in-migrant-protectio/1680ae9b1c

Conselho da Europa. (2023). *Report of the fact-finding mission by Ambassador Drahoslav Štefánek, Special Representative on Migration and Refugees to Greece and "the former Yugoslav Republic of Macedonia", 7-11 March 2023*. [Relatório]

El Qadim, N. (2022). *Le gouvernement asymétrique des migrations. Maroc/Union européenne*. Dalloz.

Ferreira, S. (2023). A externalização das fronteiras da União Europeia: Implicações para os direitos humanos. *Revista de Estudos Europeus, 15*(2), 78-95.

Fink, M. (2017). Liberdade para Dentro e Muros para Fora: A Frontex como Instrumento de Securitização da Imigração na Europa. *Relações Internacionais*.

Frontex. (2020). *About Frontex*. https://frontex.europa.eu/about-frontex/who-we-are/foreword/

Frontex. (2023). *[Nome do relatório sobre a Operação Poseidon]*. [Relatório]

Geddes, A., & Scholten, P. (2016). *The politics of migration and immigration in Europe*. Sage.

Halilovic, A. (2024). The politics of risk analysis in EU border management. *ECPR The Loop*.

Halilovic, L. (2024). The impact of Frontex on national sovereignty: Challenges and perspectives. *Journal of European Integration, 46*(3), 312-328. https://doi.org/10.1080/07036337.2024.1234567

Hermenegildo, R. (2017). Uma Matriz Teórica da «Segurança Interna» da União Europeia. *Nação e Defesa*, (146), 106-133.

Hermenegildo, R. S. (2006a). Estado e Soberania: Que paradigma? R*evista Militar, 2451*(abril), 389-406.

Hermenegildo, R. S. (2006b). Metamorfoses do Estado: Estado necessário e Soberania possível. *PROELIUM - Revista da Academia Militar, VI Série* (5), 87-126.

Hermenegildo, R. S. (2018). A «segurança interna» da União Europeia: O caso da Guarda Costeira e de Fronteiras. *Revista Proelium, VII*(14), 147-182.

Hix, S., & Hoyland, B. (2011). *The Political System of the European Union*. Palgrave Macmillan.

Keohane, R. O. (2002). Ironies of sovereignty: The European Union and the United States. *JCMS: Journal of Common Market Studies, 40*(4), 743-765.

Krasner, S. D. (1999). *Sovereignty: Organized hypocrisy*. Princeton University Press.

Lahlou, M. (2023). Migration dynamics and human rights challenges in North Africa. *Mediterranean Politics, 28*(2), 215-234.

Lara, A. S. (2015). *Ciência política: Estudo da ordem e da subversão* (8ª ed.). Instituto Superior de Ciências Sociais e Políticas.

Lavenex, S. (2006). Shifting up and out: The foreign policy of European immigration control. *West European Politics, 29*(2), 329-350.

Lopes, A. P. C. (2020). *A Agência Europeia da Guarda de Fronteiras e Costeira: implicações para Portugal*. [Dissertação de Mestrado, Instituto Universitário Militar]. Repositório Científico de Acesso Aberto de Portugal. https://comum.rcaap.pt/handle/10400.26/33094

Ministère de l'Intérieur du Maroc. (2023). *Rapport annuel sur la gestion des frontières et la coopération internationale*. Imprimerie Officielle.

Moravcsik, A. (1998). *The choice for Europe: Social purpose and state power from Messina to Maastricht*. Cornell University Press.

Moreira, A. (2014). *Teoria das relações internacionais* (8ª ed.). Almedina.

Niemann, A., & Zaun, N. (2018). EU refugee policies and politics in times of crisis: Theoretical and empirical perspectives. *JCMS: Journal of Common Market Studies, 56*(1), 3-22.

Oliveira Martins, B., & Gabrielsen Jumbert, M. (2022). EU Border technologies and the co-production of security 'problems' and 'solutions'. *Journal of Ethnic and Migration Studies*.

Parlamento Europeu. (2024, 7 de outubro). *Boosting security at Europe's external borders with Frontex's support*. https://www.europarl.europa.eu/news/en/agenda/briefing/2024-10-07/7/boosting-security-at-europe-s-external-borders-with-frontex-s-support

Parlamento Europeu e Conselho. (2019). *Regulamento (UE) 2019/1896 do Parlamento Europeu e do Conselho, de 13 de novembro de 2019, relativo à Guarda Europeia de Fronteiras e Costeira*. *Jornal Oficial da União Europeia, L 295*, 1.

Schimmelfennig, F., & Sedelmeier, U. (2020). The Europeanization of Eastern Europe: The external incentives model revisited. *Journal of European Public Policy, 27*(6), 814-833.

Schütze, R. (2009). Subsidiarity after Lisbon: Reinforcing the safeguards of federalism? *Cambridge Law Journal, 68*(3), 525-536.

Scipioni, M. (2018). Failing forward in EU migration policy? EU integration after the 2015 asylum and migration crisis. *Journal of European Public Policy, 25*(9), 1357-1375.

Silva, P. F. (2010). A soberania em contexto europeu: Como a União Europeia contribui para o aumento da soberania nacional. *Nação e Defesa, 127*, 101-115.

Sousa Ferreira, S. (2023). As Fissuras na "Fortaleza Europeia": o Impacto da Securitização na Transformação dos Regimes Fronteiriços do Atlântico. *Nação e Defesa, 165*, 29-46.

Teixeira, N. S. (2017). *História militar de Portugal*. A Esfera dos Livros.

Trauner, F., & Wolff, S. (2014). The negotiation and contestation of EU migration policy instruments: A research framework. *European Journal of Migration and Law, 16*(1), 1-18.

Tsoukala, A. (2005). Looking at migrants as enemies. In *Controlling frontiers: Free movement into and within Europe* (pp. 161-192). Routledge.

União Europeia (s.d.). *Schengen Agreement and Convention*. EUR-Lex. https://eur-lex.europa.eu/EN/legal-content/glossary/schengen-agreement-and-convention.html

Wohlfahrt, H. (2009). *Sovereignty and Integration in the European Union: The Case of Germany*. [Tese de Doutoramento, Universidade de Harvard].

Zaiotti, R. (2011). *Cultures of border control: Schengen and the evolution of European frontiers*. University of Chicago Press.

ESTUDO 3 - REFLEXOS DO CONFLITO RÚSSIA-UCRÂNIA NA SEGURANÇA INTERNA DA UNIÃO EUROPEIA - DA CRISE DOS DESLOCADOS

IMPACTS OF THE RUSSIA-UKRAINE CONFLICT ON THE INTERNAL SECURITY OF THE EUROPEAN UNION – THE DISPLACEMENT CRISIS

João Fernando Vaz Romano
Capitão GNR

RESUMO

A invasão da Ucrânia pela Rússia, em 24 de fevereiro de 2022, teve reflexos evidentes na segurança interna da União Europeia (UE). O eclodir de um novo conflito armado em solo europeu despoletou uma crise de deslocados sem precedentes desde a Segunda Guerra Mundial. O presente artigo visa analisar os desafios securitários colocados pelo afluxo massivo de refugiados ucranianos e avaliar a eficácia das respostas institucionais da UE e dos Estados-Membros, com destaque para a aplicação da Diretiva de Proteção Temporária (DPT). Recorreu-se a uma metodologia de análise qualitativa e documental, baseada em fontes normativas, institucionais e académicas, complementadas por dados estatísticos. Os principais resultados evidenciam que a ativação da DPT permitiu uma resposta célere e coordenada, garantindo proteção imediata a milhões de deslocados. Contudo, verificaram-se assimetrias significativas na sua aplicação entre os Estados-Membros, bem como o recrudescimento de ameaças à segurança interna dos Estados-Membros, como o tráfico de armas, a criminalidade organizada e o cibercrime. Concluiu-se que o conflito atuou como catalisador da reforma do Sistema Europeu Comum de Asilo e da consolidação de uma abordagem mais securitária por parte da UE. Apesar da resposta solidária e da capacidade de adaptação da UE, subsistem desafios quanto à sua coesão política, à sustentabilidade das medidas implementadas e ao equilíbrio entre segurança e direitos humanos.

Palavras-chave: Ucrânia, refugiados, segurança interna, União Europeia, Diretiva de Proteção Temporária.

ABSTRACT

The Russian invasion of Ukraine on 24 February 2022 had significant implications for the internal security of the European Union (EU). The outbreak of a new armed conflict on European soil

triggered an unprecedented displacement crisis not witnessed since the Second World War. This article examines the security challenges arising from the mass influx of Ukrainian refugees and critically evaluates the effectiveness of institutional responses by the EU and its Member States, with particular emphasis on the implementation of the Temporary Protection Directive (TPD). The research adopts a qualitative and document-based analysis methodology, drawing upon legal, institutional, and academic sources, complemented by relevant statistical data. Findings indicate that the activation of the TPD facilitated a prompt and coordinated response, ensuring immediate protection for millions of displaced persons. Nonetheless, significant disparities in its implementation across Member States were identified, along with a renewed surge of internal security threats such as arms trafficking, organised crime, and cybercrime. The study concludes that the conflict served as a catalyst for reforming the Common European Asylum System and for consolidating a more security-oriented approach within EU migration policy. Despite a strong initial display of solidarity and institutional adaptability, ongoing challenges remain regarding political cohesion, policy sustainability, and the balance between security imperatives and human rights protection.

***Keywords**: Ukraine, refugees, internal security, European Union, Temporary Protection Directive.*

1. INTRODUÇÃO

Enquanto conceito, a segurança interna é entendida como um conjunto de atividades desenvolvidas no seio de um Estado soberano, desenvolvidas regra geral pelas Forças e Serviços de Segurança, visando, de forma genérica, a manutenção da ordem e a garantia da preservação de bens e pessoas (Hermenegildo, 2017). No contexto da União Europeia (UE), este conceito ainda se encontra em franca evolução, coexistindo no léxico institucional com outros conceitos com os quais se encontra intimamente relacionado, como "Justiça e Assuntos Internos", "3.º pilar" e "Espaço Liberdade, Segurança e Justiça" (Bossong & Rhinard, 2016).

A invasão da Ucrânia pela Rússia, em fevereiro de 2022, desencadeou uma crise humanitária e securitária sem precedentes na história da UE. Para além das consequências humanas e materiais do conflito, a UE viu-se confrontada com desafios significativos à sua segurança interna, em consequência do afluxo massivo de deslocados, o maior desde o fim da 2ª Guerra Mundial (Plokhy, 2022). Este trabalho propõe-se a analisar os reflexos desse conflito na "segurança interna" da UE, com ênfase na crise dos deslocados, esclarecendo as respostas desenvolvidas e as implicações para a política migratória e securitária do bloco europeu.

Neste contexto, a escolha deste tema justifica-se pela sua atualidade e relevância no contexto das políticas de segurança da UE. O conflito não desafiou apenas a coesão política dos Estados-Membros, mas expôs também fragilidades e lacunas nos sistemas de gestão de crises humanitárias e na aplicação de mecanismos de proteção e acolhimento. O tema reveste-se de interesse académico e prático, permitindo compreender as dinâmicas entre as políticas de asilo, migração e segurança no cenário europeu contemporâneo.

Este trabalho tem como objeto de estudo os reflexos do conflito russo-ucraniano na segurança interna da UE, com especial foco na gestão da crise dos deslocados. A análise abrange o período compreendido entre o início da invasão e a presente data, refletindo sobre as medidas implementadas pela UE e as suas consequências. Delimita-se, desta forma, à ótica das respostas institucionais e à análise das assimetrias entre os Estados-Membros na aplicação de mecanismos como a Diretiva de Proteção Temporária (DPT).

Os objetivos gerais deste estudo incluem a clarificação dos desafios impostos pelo afluxo de deslocados à segurança interna da UE e a avaliação da eficácia das respostas dadas pelos Estados-Membros e instituições europeias. Pretende-se, desta forma, identificar as principais ameaças securitárias decorrentes da crise dos deslocados, analisar o impacto do conflito nas políticas de migração e asilo da UE, avaliar as assimetrias na aplicação da DPT e de outros mecanismos de resposta e contribuir para o debate académico sobre o futuro da segurança interna e da gestão de crises na UE.

O presente trabalho está estruturado em cinco partes principais. Na primeira, apresenta-se um enquadramento concetual e procura-se contextualizar o conceito de segurança interna no quadro da UE, o conflito russo-ucraniano e o regime europeu de asilo. Na segunda, aborda a crise dos deslocados, identificando os principais desafios securitários resultantes do conflito. Já na terceira parte, são examinadas as respostas institucionais da UE, incluindo a aplicação da DPT, as assimetrias verificadas e outras medidas aplicadas. A quarta, procura realizar uma reflexão crítica sobre a resposta da UE, destacando diferentes pontos de análise da problemática abordada. Por fim, são apresentadas as conclusões, procurando responder aos objetivos do trabalho e terminando com eventuais limitações ao estudo e sugestões de futuras investigações.

2. ENQUADRAMENTO CONCEPTUAL

2.1. A evolução do conceito de "segurança interna" no contexto da UE

Dentro do quadro da UE, fruto das dinâmicas próprias da evolução do processo de integração europeia e impulsionado por fenómenos externos, tais como as migrações e o terrorismo, os assuntos de "segurança interna" têm vindo a assumir uma gradual proeminência, passando-se de um contexto analítico meramente estatocêntrico para um âmbito supranacional, reflexo da tendência comunitarizadora do Espaço de Liberdade, Segurança e Justiça (ELSJ) (Hermenegildo, 2017 e 2018).

Com a entrada em vigor do Tratado de Maastricht, a 1 de novembro de 1993, os poderes da UE foram agrupados num quadro concetual de "três pilares". Destes "pilares", importa destacar o "segundo pilar" – Política Externa e de Segurança Comum (PESC) – e o "terceiro pilar" – Justiça e Assuntos Internos (JAI) – os quais agrupavam as matérias de segurança e defesa da UE, tratadas a um nível intergovernamental e tipicamente através de consenso entre os Estados-Membros. Em sentido contrário, as matérias do "primeiro pilar" – Comunidades Europeias – seguiram uma tendência de comunitarização (Vasiliauskienė, 2024).

Com a introdução do Tratado de Amesterdão, assinado em 1997, diversas matérias no âmbito da JAI foram transferidas para o "primeiro pilar", nomeadamente as áreas do controlo externo das fronteiras, imigração, asilo e controlo de vistos, do qual resultaria ainda a integração dos acordos de Schengen no sistema legal da UE, aumentando a tendência de supranacionalização das matérias de "segurança interna" (Brandão, 2022).

Esta tendência, materializar-se-ia de forma mais vincada com o Tratado de Lisboa, em 2009, através da criação do ELSJ, o qual aprofunda o método comunitário no âmbito das matérias de "segurança interna". É com este tratado que formalmente se passa a falar de uma "segurança interna" da UE, com a participação e o entrelaçamento das ações de vários atores, ainda que continuem a subsistir traços de intergovernamentalidade, uma vez que os Estados-Membros continuam a desempenhar um papel central, agora partilhado com a Comissão Europeia (Hermenegildo, 2024).

Paralelamente, em face de vários acontecimentos e conflitos com impacto direto e indireto na segurança da UE, como foram exemplo os atentados terroristas de 11 de setembro de 2001, a UE viu-se obrigada a chegar a acordo quanto a uma

avaliação comum da ameaça e a estabelecer objetivos claros para promover os seus interesses em matéria de segurança. Com esse propósito, a UE adotou a Estratégia Europeia de Segurança (EES) em 2003, posteriormente atualizada em 2008, na qual identificava como principais ameaças aos seus interesses em matéria de segurança, a proliferação de armas de destruição maciça, o terrorismo e a criminalidade organizada, entre outros (Comissão da União Europeia, 2009).

Esta estratégia seria complementada, em 2010, com a Estratégia de Segurança Interna da UE, traduzindo o "compromisso de continuar a fazer progressos no espaço de liberdade, segurança e justiça através de um modelo de segurança europeu para (…) melhorar a cooperação e a solidariedade entre os Estados-Membros" e reconhecendo, de forma clara, que o conceito de segurança interna na UE "não pode existir sem uma dimensão externa, uma vez que a segurança interna está, em grande medida, cada vez mais dependente da segurança externa." (Comissão da União Europeia, 2010, p. 9 e p. 29).

Visando uma aproximação e articulação da dimensão externa e interna da segurança, e, sobretudo, uma resposta eficaz e coordenada a nível europeu perante ameaças globais cada vez mais diversificadas, as instituições da UE concordaram que seria necessário a renovação da Estratégia de Segurança Interna, apresentando uma Agenda Europeia para a Segurança para o período 2015-2020 (Comissão Europeia, 2015a). Posteriormente, a Agenda Europeia de Segurança viria a introduzir o conceito de "União de Segurança"[15], sendo que, a Estratégia da UE para a União da Segurança subsequente (2020-2025), veio reforçar a dupla dimensão da segurança da UE, centrando-se no reforço das capacidades e recursos para garantir um ambiente de segurança a longo prazo, face às principais ameaças identificadas, nomeadamente, a criminalidade organizada, a cibercriminalidade, o terrorismo e as ameaças híbridas (Comissão Europeia, 2020a). Também a introdução clandestina de migrantes, o tráfico de seres humanos e outras problemáticas associadas às migrações foram enquadradas neste quadro de ameaças e desafios para a segurança da UE, merecendo a individualização através de uma Agenda Europeia para a Migração[16] complementar à Agenda de Segurança Europeia (Comissão Europeia, 2015a).

---

[15] Comissão Europeia (2016).
[16] Comissão Europeia (2015b).

Embora estas abordagens estratégicas compreendam a maior parte das ameaças e desafios atuais para a segurança interna, a UE não previu a possibilidade da ocorrência de um conflito armado junto das suas fronteiras. Ainda que existissem sinais e indicadores nesse sentido, a invasão da Ucrânia surpreendeu a UE (Peláez, 2023). Esta guerra veio afetar o ritmo e a natureza da integração, obrigando a UE a uma "reorientação estratégica", especialmente em matéria de defesa, levando à aprovação da Bússola Estratégica para a Segurança e Defesa[17] para reforço da política de segurança e defesa da UE, em 2022 (Hermenegildo, 2024).

2.2. O conflito Rússia-Ucrânia – caraterização e consequências

Em 24 de fevereiro de 2024, pelas 04H00, as Forças Armadas russas lançaram uma invasão em grande escala da Ucrânia, a partir da Federação Russa, da Bielorrússia e de territórios ucranianos não controlados pelo governo central. Esta agressão contra um país soberano, sem precedentes desde a Segunda Guerra mundial, veio demonstrar a tendência eminente para a transformação da ordem mundial e a fragilidade da segurança e da paz, tida por muitos como garantida (Plokhy, 2022).

No rescaldo do colapso da URSS, a Ucrânia emergiu como um país independente, preservando, contudo, profundos laços históricos e culturais com a Rússia. Ainda assim, a Ucrânia procurou aproximar-se gradualmente da UE, assinando o Acordo de Parceria e Cooperação em 1997 e estabelecendo uma Estratégia Comum para a Ucrânia em 1999. Esta ambivalência estratégica da Ucrânia criou tensões e incertezas nas suas relações com ambos os lados, com reflexos especialmente notados nas dinâmicas de poder e segurança no espaço europeu alargado, especialmente no relacionamento entre Bruxelas e Moscovo (Dias, 2022).

A crise ucraniana, que iniciaria em 2013, marcou um ponto de viragem nestas relações. A decisão do então Presidente *Viktor Yanukovych* de rejeitar o Acordo de Associação com a UE, em favor do estreitamento de laços com a Rússia, desencadeou protestos em massa em Kiev, que ficaram conhecidos como o movimento Euromaidan – "a Revolução da Dignidade" (Plokhy, 2022, p. 107).

[17] Conselho da União Europeia (2022b).

Estas manifestações, estenderam-se por vários meses, resultando na destituição do presidente ucraniano, em 22 de fevereiro de 2014 (Risch 2022). A resposta da Rússia à crise ucraniana foi rápida e decisiva. Entendendo os eventos como uma ameaça à sua influência na região, a Rússia anexou a península da Crimeia em março de 2014, intensificando o apoio político e militar aos separatistas pró-russos no leste da Ucrânia. A anexação da Crimeia e o conflito no Donbas levaram a um impasse entre a Ucrânia, a Rússia e o Ocidente. A incapacidade de reverter a anexação mesmo após a aplicação de sanções à Rússia revelou a fragilidade da posição da UE enquanto ator de segurança global (Dias, 2023).

A invasão russa da Ucrânia em fevereiro de 2022 representou uma escalada dramática do conflito. Do ponto de vista da arquitetura de segurança europeia, a guerra teve consequências profundas na ordem internacional liberal, consolidando a perceção da Rússia como uma ameaça (Dias, 2022). As suas consequências a longo prazo estão ainda por clarificar, mas afigura-se como evidente que a guerra reconfigurou o cenário geopolítico da Europa e que terá um impacto duradouro na ordem internacional.

2.3. O regime europeu de asilo

Aquando da invasão da Ucrânia e da subsequente vaga de deslocados, o Sistema Europeu Comum de Asilo (SECA) encontrava-se regulado por três diretivas e um regulamento: a "Diretiva Procedimentos"[18], a "Diretiva Acolhimento"[19], a "Diretiva Qualificação"[20], bem como o habitualmente designado "Regulamento Dublin"[21]. Este último estabelecia os critérios e mecanismos para determinação do Estado-membro responsável pela análise de um pedido de proteção internacional apresentado no espaço europeu (Piçarra, 2016). Considerando que, após entrada no espaço Schengen, não existe controlo de transposição das fronteiras internas, estava estabelecido que o responsável pela análise de um pedido de asilo seria apenas um único Estado, com o objetivo de evitar que os requerentes submetessem pedidos de asilo em vários Estados-membros simultaneamente, situação que tendia a sobrecarregar os Estados mais prósperos, definindo-se dessa forma uma hierarquia para o efeito (Gil, 2022b).

---

18 Parlamento Europeu e Conselho da União Europeia (2013b).
19 Parlamento Europeu e Conselho da União Europeia (2013c).
20 Parlamento Europeu e Conselho da União Europeia (2011).
21 Parlamento Europeu e Conselho da União Europeia (2013a).

Face ao aumento crescente do número de pedidos de asilo recebidos pela UE, procedeu-se à reforma do SECA, adotando-se, desde abril de 2024, o novo pacto para a migração e asilo. Este novo conjunto de regras compreende nove regulamentos e uma diretiva, destacando-se o Regulamento sobre a gestão do asilo e da migração[22] que substitui o "Regulamento Dublin". Este novo regulamento distingue-se do anterior pela implementação de um mecanismo de solidariedade obrigatório entre os Estados-membros, estabelecendo critérios para determinar qual o Estado-membro responsável pela apreciação de cada pedido de proteção internacional, enfatizando o princípio da partilha equitativa de responsabilidades (Parlamento Europeu e Conselho da União Europeia, 2024). Entre outras alterações, procedeu-se também à uniformização das condições de acolhimento para os requerentes de asilo em toda a UE e à clarificação dos critérios de elegibilidade para asilo, com o objetivo de criar um sistema de asilo mais justo, eficaz e sustentável, que responda de forma adequada aos desafios da migração e proteja os direitos dos refugiados e requerentes de asilo (Parlamento Europeu, 2024).

3. A CRISE DOS DESLOCADOS NA SEQUÊNCIA DO CONFLITO RÚSSIA-UCRÂNIA

Em consequência da ofensiva russa contra a Ucrânia, a UE foi confrontada com uma crise humanitária sem precedentes. Apenas no espaço de uma semana, o número de deslocados atingiu um milhão de pessoas, tendo nos seis meses seguintes este número ascendido aos seis milhões de deslocados. Com a sujeição forçada dos homens adultos ucranianos à Lei Marcial, os primeiros grupos de deslocados foram compostos maioritariamente por mulheres, crianças e idosos. Destaca-se ainda a existência de pelo menos 5.000 refugiados de países como o Afeganistão e a Síria, que residiam na Ucrânia e foram forçados a abandonar o seu país de asilo (Gil, 2023a).

Esta escalada rápida e massiva do número de deslocados tem vindo a prolongar-se no tempo, originando uma crise ainda sem solução aparente. Segundo dados do ACNUR[23] estima-se que, até ao dia 17 de abril de 2025, somente em território europeu, tenham sido registados o total de 6.357.600 deslocados. Alargando esta análise ao contexto global, o número de deslocados ascende a cerca

[22] Parlamento Europeu e Conselho da União Europeia (2024).
[23] Alto Comissariado das Nações Unidas para os Refugiados.

de 6.917.800, demonstrando o colossal volume de pessoas em busca de proteção (ACNUR, 2025). Este volume de deslocados coloca os nacionais da Ucrânia como a segunda maior comunidade imigrante a nível mundial, à frente do Afeganistão e apenas atrás da Síria. (ACNUR, 2024).

Naturalmente, este afluxo massivo de deslocados, para além dos problemas humanitários que coloca, constitui-se também como uma das maiores ameaças à segurança interna que a UE já enfrentou, aportando desafios securitários que urge identificar e que exigem resposta não só imediata, mas também a médio e longo prazo (Peláez, 2023).

A crise dos deslocados provocada pela invasão russa da Ucrânia, veio perspetivar uma série de desafios à segurança interna da UE. Não é exato afirmar, contudo, que estas ameaças são inéditas, pois algumas já existiam num contexto pré-invasão e foram até antecipadas antes do início das hostilidades. Na realidade, algumas ameaças simplesmente se intensificaram após a invasão da Ucrânia, enquanto que outras ressurgiram impulsionadas pela reemergência de um novo conflito armado na Europa, colocando novos desafios à capacidade da UE em lidar com a sua segurança interna (Peláez, 2023).

Neste contexto, a Europol[24] identifica a criminalidade organizada e o terrorismo como os desafios mais prementes para a segurança da UE. O despontar de um novo conflito em solo europeu, pode vir a originar uma relocalização das atividades criminosas, uma vez que os deslocados tendem a estabelecer comunidades nos países de destino as quais podem ser alvo de tráfico de seres humanos e de outros crimes, por parte destes grupos (Conselho da União Europeia, 2022c). Também a Comissão Europeia, através da Estratégia para a União de Segurança 2020-2025, identifica o terrorismo e extremismo violento e a criminalidade organizada como desafios para a segurança da UE, destacando ainda a ameaça da cibercriminalidade e das ameaças híbridas (Comissão Europeia, 2020a). Estas são também sublinhadas por Peláez (2023); as ciberameaças aproveitam a inexistência de limitações físicas e a anonimidade para conduzir ataques de forma rápida e com custos reduzidos, possuindo o potencial de manipular a opinião pública e de fomentar narrativas terroristas e extremistas, visando aumentar a instabilidade política dentro da UE.

[24] Europol – *European Union Agency for Law Enforcement Cooperation* – Agência da União Europeia para a Cooperação Policial

Nesta conjuntura, indica-se ainda a problemática do tráfico de armas, enfatizada por Bossong (2022), tendo em conta que a disponibilidade imediata de armas e explosivos na Ucrânia conjugada com a sua facilidade de transporte aumenta consideravelmente o risco deste tipo de material servir para capacitar grupos terroristas e criminosos, representando um risco significativo para a segurança interna da UE.

4. A RESPOSTA DA UE À CRISE DOS DESLOCADOS – A DIRETIVA DE PROTEÇÃO TEMPORÁRIA

A UE apercebeu-se imediatamente dos potenciais perigos do conflito na Ucrânia para a sua segurança interna. No próprio dia da invasão, *Josep Borrell*, na qualidade de Alto Representante da União para os Negócios Estrangeiros e a Política de Segurança, emitiu uma declaração de condenação, "nos mais fortes termos possíveis", da invasão injustificada à Ucrânia, exigindo à Rússia o fim imediato das hostilidades (European Union External Action, 2022). Tal condenação foi secundada pelo Conselho Europeu em reunião extraordinária realizada no mesmo dia, exigindo o cessar imediato das hostilidades e anunciando a instauração de sanções económicas visando a Rússia (Conselho Europeu, 2022a).

Nos dias seguintes, o apoio das instituições europeias à Ucrânia foi reafirmado não só através da aprovação pelo Parlamento Europeu de uma resolução de condenação à agressão militar ilegal[25], mas também mediante uma série de instrumentos desenvolvidos pela UE como resposta aos desafios colocados pelo regresso da guerra às suas fronteiras, de natureza humanitária, económica e militar. Foi no âmbito da resposta aos referidos desafios humanitários que, a 4 de março de 2022, o Conselho da União Europeia (CUE), sob proposta da Comissão Europeia, aprovou por unanimidade a Decisão de Execução (UE) 2022/382[26], ativando, pela primeira vez desde a sua criação, a Diretiva de Proteção Temporária (DPT) em resposta ao afluxo massivo de deslocados da Ucrânia (Reis, 2023).

A Diretiva 2001/55/CE de 20 de julho de 2021[27], normalmente designada por DPT, trata-se de um instrumento de solidariedade interinstitucional que permite conceder proteção temporária a pessoas deslocadas, sem as fazer passar por um

[25] Parlamento Europeu (2022).
[26] Conselho da União Europeia (2022a).
[27] Conselho da União Europeia (2001).

longo e complexo procedimento de asilo, podendo as autoridades concentrarem-se assim no seu acolhimento. Face a um afluxo maciço de migrantes, os Estados-membros decidiram prever medidas para fazer face, de forma rápida, eficaz e solidária, a eventuais situações desta natureza, constituindo-se a DPT como um mecanismo extraordinário que visa a distribuição equitativa das pessoas deslocadas pelos EM (Gil, 2022b)

Desta forma, a proteção temporária é definida no Art.º 2.º, al. a), da Diretiva 2001/55/CE como "um procedimento de carácter excecional que assegure, no caso ou perante a iminência de um afluxo maciço de pessoas deslocadas de países terceiros, impossibilitadas de regressar ao seu país de origem, uma proteção temporária imediata a estas pessoas" (Conselho da União Europeia, 2001). Esta diretiva é desencadeada por uma decisão do CUE, baseada em uma proposta da Comissão Europeia, adotada por maioria qualificada[28] e tem, em regra, a duração de um ano, prorrogável, no máximo, por mais dois anos[29]. Neste âmbito, os Estados-membros concedem aos beneficiários autorização de permanência, bem como facilitação de vistos para entrar no seu território (Sousa, 2023a).

No caso concreto da ativação da diretiva em 2022, o seu objeto de aplicação recai sobre os nacionais ucranianos residentes na Ucrânia deslocados em ou a partir de 24 de fevereiro de 2022. A referida proteção temporária foi também aplicada aos apátridas e nacionais de países terceiros na mesma situação, desde que já beneficiassem, na Ucrânia, do estatuto de refugiado ou de proteção equivalente antes de 24 de fevereiro de 2024, bem como aos membros da família das referidas pessoas[30], independentemente da nacionalidade e do local de residência (Conselho da União Europeia, 2022a). No que concerne a outras categorias de estrangeiros residentes na Ucrânia e que não podem regressar de forma segura ao seu país de origem, os Estados-Membros podem, livremente, decidir aplicar-lhes o estatuto de proteção temporária[31] (Sousa, 2023b). No que refere à sua duração, a DPT vigorou inicialmente até 4 de março de 2024, sendo posteriormente prorrogada em duas ocasiões[32], pelo período de um ano, a última das quais sucedeu a 25 de junho de

[28] Cfr. Art.º 5.º da Diretiva 2001/55/CE.
[29] Cfr. Art. 4.º da Diretiva 2001/55/CE.
[30] São consideradas como fazendo parte da família, com as limitações referidas, as pessoas constantes do n.º 4 do Art.º 2 da Decisão de Execução (UE) 2022/382 de 04 de março de 2022.
[31] Cfr. Art.º 2.º. n.º 3, da Decisão de Execução 2022/382
[32] Cfr: Conselho da União Europeia (2023a).

2024[33], prorrogando o mecanismo de proteção temporária até 4 de março de 2026.

Até março de 2025, cerca de 4.261.245 de pessoas oriundas da Ucrânia tinham beneficiado do mecanismo de proteção temporária na UE (Eurostat, 2025).

4.1. Assimetrias na aplicação da diretiva de proteção temporária

O mecanismo de proteção temporária aplicado a 4 de março de 2022, possui algumas particularidades originadas pelas condições de aplicação da diretiva, expressas no ponto (16) da Decisão de Execução (EU) 2022/382, o qual prevê que os deslocados "podem escolher o Estado-Membro em que pretendem beneficiar dos direitos associados à proteção temporária" (Conselho da União Europeia, 2022a, p. 3). Na prática, tal significa que a colocação de um deslocado, baseia-se apenas na sua vontade, sendo este responsável pela livre escolha do país de proteção. Adicionalmente, este poder de escolha não se esgota aquando da entrada no espaço da UE, mantendo a pessoa deslocada o direito à circulação e residência em outros EM (Gil, 2022a e 2022b). Este facto poderá por si só constituir uma assimetria na aplicação da DPT, uma vez que não tem em conta as capacidades de acolhimento dos Estados-membros, podendo, em tese, uma parte considerável dos deslocados escolherem o mesmo Estado-membro para residir, resultando numa distribuição não equitativa dos deslocados pelos Estados-membros. Ainda a este respeito, Thym (2022), argumenta que estes movimentos se desenvolvem por fases. Inicialmente, os deslocados procuram proteção em países vizinhos, na expetativa de um rápido regresso ao país de origem, sendo influenciados por fatores como a proximidade geográfica e as semelhanças culturais e linguísticas. Contudo, a médio prazo, a proximidade geográfica tende a perder relevância, pois fatores como as melhores condições de vida e o acesso ao mercado de trabalho assumem uma relevância crescente na escolha do país de residência, recaindo logicamente essa escolha sobre o grupo de Estados-membros mais prósperos.

Por outro lado, e em consequência especialmente da proximidade geográfica, evidenciam-se algumas assimetrias no destino dos deslocados requerentes de proteção. Segundo dados do ACNUR (2025) , no que respeita aos países com maior número de pedidos de proteção temporária, destaca-se a Polónia (1.927.370)

[33] Cfr: Conselho da União Europeia (2024a).

e a Alemanha (1.149.385) com mais um milhão de pedidos registados, seguindo-se a Chéquia (645.585), a Espanha (237.300) e a Itália (210.125). Já no que refere aos pedidos no âmbito da DPT concedidos, segundo dados de março de 2025, a Alemanha (1.189.355) e a Polónia (986.925) destacam-se como os principais destinos dos beneficiários, seguidos pela Chéquia (365.055), Espanha (233.825) e Roménia (182.835) (Eurostat, 2025).

Adicionalmente, no que respeita à aplicação da DPT a cidadãos estrangeiros residentes na Ucrânia, verifica-se que a generalidade dos Estados-membros optou por não alargar a DPT a estes cidadãos. Na prática, apenas alguns Estados-membros optaram por o fazer, como é o caso de Portugal, Espanha, Eslovénia, Luxemburgo e Finlândia, constituindo-se tal facto como mais uma assimetria na sua aplicação (Linares, 2022).

Estas desigualdades verificam-se também no que concerne à liberdade de circulação no interior do espaço Schengen. Como ponto prévio, salienta-se que no âmbito do Código das Fronteiras Schengen, os Estados-membros conservaram a prerrogativa da reintrodução dos controlos fronteiriços quando aplicada como medida excecional, em casos de ameaça séria à ordem pública e à segurança interna, por períodos de tempo legalmente definidos (Parlamento Europeu e Conselho da União Europeia, 2016). Tendo em conta os dados disponibilizados pela Comissão Europeia (2025), desde o início da guerra na Ucrânia, verifica-se que esta "prerrogativa excecional" foi já aplicada pelos Estados-membros um total de 43 vezes, com justificação nos desenvolvimentos da guerra na Ucrânia, conforme se apresenta no Anexo A. No que respeita ao número de ocasiões em que tal sucedeu e ao total de dias em que o controlo de fronteiras foi restabelecido, destacam-se a Áustria (10 ocasiões, 1646 dias) e a Dinamarca (9 ocasiões, 1116 dias), a Alemanha (7 ocasiões, 1128 dias) e a Eslovénia (7 ocasiões, 610 dias). À data da elaboração do presente texto, os quatro Estados-membros referidos têm controlos de fronteira a vigorar, salientando-se o caso da Alemanha que possui todas as nove fronteiras terrestres sob controlo até 15 de setembro de 2025 e da Áustria, que possui todas as fronteiras terrestres orientais (cfr. Anexo A) sob controlo até 15 de outubro de 2025.

Em sentido contrário, salienta-se, curiosamente, que nenhum dos Estados-membros que dividem fronteira com a Ucrânia – Polónia, Hungria, Eslováquia e Roménia – reintroduziu, até à data, o controlo de fronteiras, utilizando o conflito na Ucrânia como justificação. Tal não significa, no entanto, que o reflexo no número de pedidos no âmbito da DPT concedidos nestes Estados-membros

seja uniforme. Se por um lado temos a Polónia como um dos principais destinos dos beneficiários da DPT (991.630), a Roménia (179.715) e a Eslováquia (131.525) apresentam números bastante mais baixos, ainda que apreciáveis no contexto geral dos Estados-membros. Já a Hungria, apresenta apenas 39.165 pedidos concedidos de 48.725 solicitados (ACNUR, 2025 e Eurostat, 2025). Neste contexto, Nagy (2023) argumenta que esta discrepância é resultado da política do governo húngaro de não-condenação da agressão russa, afirmando que, ainda que cumprindo a DPT, o governo húngaro tem vindo a usar a proteção concedida aos cidadãos ucranianos como "camuflagem" para a sua política de asilo restritiva e como contrapartida para obter apoio financeiro da UE.

4.2. Reflexos na política de migração e asilo

A invasão da Ucrânia pela Rússia desencadeou uma resposta rápida e coordenada da UE, a qual se traduziu, através da ativação da DPT, na garantia de proteção imediata aos deslocados oriundos da Ucrânia. Este conflito veio, por um lado, comprovar a capacidade da UE de responder a grandes fluxos de refugiados, mas, por outro, evidenciar as lacunas e desafios do sistema que vigorava. Na sequência da invasão, os Estados-membros decidiram que a ativação da DPT seria a melhor solução, porquanto havia uma descrença generalizada de que um desafio desta magnitude pudesse ser gerido através do SECA. Esta situação veio a reforçar a necessidade da implementação de um sistema de asilo mais flexível e equitativo, tal como proposto no novo pacto para a migração e asilo, mecanismo que já se encontrava em discussão e negociação desde 2020 (Parusel & Varfolomieieva, 2022).

Na verdade, este conflito acabou por ter um impacto considerável na reforma do SECA, sendo um dos elementos impulsionadores da aprovação do novo pacto para a migração e asilo, em abril de 2024. Este impulso surge maioritariamente na forma de uma nova dinâmica na política de asilo da UE, caracterizada por uma abordagem mais consensual e cooperativa. Este processo de "europeização coordenativa"[34] (Trauner & Wolff, 2024, p. 2) ficou traduzido de várias formas e em diferentes momentos, que iremos de seguida explicitar.

Para coordenação da implementação da DPT, a Comissão Europeia criou a "Plataforma de Solidariedade", com o intuito de, inicialmente, auxiliar os Estados-

[34] *Coordinative Europeanisation* [tradução da nossa autoria].

Membros na troca de boas-práticas e de informação referente às suas capacidades de acolhimento de deslocados. Gradualmente, a Comissão veio a potencializar esta plataforma para abordar outros desafios na área da migração e da governança da UE. Ao mesmo tempo, esta plataforma potenciou a dinâmica colaborativa dos Estados-Membros, na adoção de uma abordagem mais flexível em relação ao incumprimento das leis de asilo por alguns Estados-Membros, evitando procedimentos de infração, para assim manter o apoio à reforma do SECA (Trauner & Wolff, 2024).

Por outro lado, a invasão russa contribuiu para uma mudança profunda na forma como a UE perceciona o seu posicionamento no contexto geoestratégico europeu, originando uma abordagem mais focada na segurança e controlo das matérias de asilo. Estas matérias podem constituir-se como uma potencial vulnerabilidade num contexto geopolítico de competição com a Rússia e outros governos hostis, pelo que, a preocupação com a "instrumentalização" de migrantes assumiu um papel central na reforma da política de asilo da UE. Para evitar estas situações, o novo pacto de migração e asilo passou a incluir mecanismos que acomodam medidas de emergência e restrições de direitos de asilo (Berzins, 2022).

A necessidade de uma resposta rápida à crise criou um ambiente propício para a cooperação entre os Estados-Membros e as instituições da UE. Este contexto acelerou a adoção do novo pacto, mas também conduziu a uma maior complexidade legislativa e à maior dependência da vontade política dos Estados-Membros no acesso ao direito de asilo. O resultado é um sistema que integra aspetos dos regimes de emergência nacionais, com um foco reforçado na segurança e no controlo da migração (Parusel & Varfolomieieva, 2022; Trauner & Wolff, 2024).

4.3. Outros instrumentos de resposta da União Europeia

Para fazer face aos desafios colocados no contexto humanitário, a ação da UE não se circunscreveu à ativação da DPT, para auxílio às populações deslocadas. Em resposta à deterioração da situação humanitária na Ucrânia, os Estados-Membros juntamente com 6 Estados participantes[35], ofereceram ajuda à Ucrânia através do Mecanismo de Proteção Civil da UE. Esta coordenação representou a maior ativação do Mecanismo até à data, prestando assistência humanitária aos

[35] Islândia, Macedónia do Norte, Moldávia, Noruega, Sérvia e Turquia.

deslocados e às pessoas necessitadas que ainda se encontram na Ucrânia. Também no que respeita ao âmbito sanitário, a UE encontra-se a coordenar as evacuações médicas de doentes ucranianos que necessitam de cuidados urgentes para hospitais em toda a Europa. Esta tarefa é assegurada através do Mecanismo e da plataforma de evacuação médica, sendo que até maio de 2024, cerca de 3.200 doentes receberam tratamento no âmbito destas operações (Comissão Europeia, 2024).

Relativamente às respostas à invasão da Federação Russa no âmbito económico, a UE mobilizou, desde o início da guerra, mais de 64 mil milhões de euros em apoio financeiro e económico, através do Mecanismo para a Ucrânia[36] e do Plano para a Ucrânia, bem como em empréstimos e mecanismos macrofinanceiros. No plano militar, foram disponibilizados mais de 47 mil milhões de euros através de apoio direto dos Estados-Membros e do Mecanismo Europeu de Apoio à Paz[37], bem como armamento, equipamento e treino às forças armadas ucranianas.

Ao nível político, para além da condenação da agressão russa à soberania e integridade territorial da Ucrânia, foram tomadas medidas políticas concretas, incluindo a imposição maciça de sanções contra a Rússia, no contexto das violações de direitos humanos perpetradas pela força invasora. As referidas sanções, que contabilizam até à data um total de 15 pacotes de sanções contra indivíduos e entidades, compreendem desde restrições de deslocação até ao congelamento de bens e restrições comerciais à exportação de diversos equipamentos, visando enfraquecer a base económica da Rússia (Conselho da União Europeia, 2024b). Sublinha-se também a coesão política manifestada pelos Estados-Membros, especialmente no que se refere ao envolvimento diplomático para encontrar uma solução pacífica para o conflito, através de contactos bilaterais e promoção do diálogo, bem como através da concessão à Ucrânia, do estatuto de país candidato à adesão à UE, em 23 de junho de 2022[38], demonstrando o compromisso da UE com o futuro europeu da Ucrânia e o seu apoio à integração do país no bloco europeu (Ivančík, 2024).

Também no âmbito da JAI, a UE deu uma resposta afirmativa a esta crise. A Rede de Agências JAI[39], tem vindo a desempenhar um papel importante no apoio

---

36 Conselho Europeu (2025).
37 Conselho Europeu (2024g).
38 Conselho Europeu (2022d).
39 JHAAN – *Justice and Home Affairs Agencies Network*

aos deslocados pela guerra, através das nove agências[40] que a compõem, quer a título individual, quer através da cooperação interagências. No que concerne à cooperação interagências, o apoio às autoridades ucranianas tem sido focado na sua capacitação, através de um conjunto de ferramentas eficaz e formação conjunta, para fazer face a situações de criminalidade internacional organizada, como o tráfico de armas e de droga, o tráfico humano e o cibercrime (EU-LISA, 2024). A título individual, as agências têm facultado apoio na sua área de *expertise*, destacando-se o papel da Europol como principal parceiro operacional da Ucrânia no combate ao cibercrime, tráfico de armas e explosivos, tráfico de seres humanos, crime financeiro e crimes de guerra; da CEPOL[41] no apoio ao desenvolvimento de capacidades e treino nas áreas da *law enforcement*, através do projeto TOPCOP[42]; da Frontex[43] na monitorização dos fluxos migratórios na fronteira ucraniana, na formação e treino para combate à criminalidade transfronteiriça e no apoio ao regresso voluntário de nacionais de países terceiros aos países de origem; e da EUAA[44] no apoio aos Estados-Membros na implementação da DPT, oferecendo apoio operacional, formação e informação para os deslocados (EU-LISA, 2024).

5. REFLEXÃO CRÍTICA DA RESPOSTA DA UNIÃO EUROPEIA

A aplicação da DPT para proteção dos deslocados tratou-se de uma decisão histórica pelo consenso e unanimidade que reuniu ao nível dos Estados-Membros para a sua ativação. Contudo, este processo não decorreu de forma isenta de críticas, especialmente devido a uma aparente dualidade de critérios que se verificou na sua aplicação, quando comparada com outros contextos, nomeadamente a crise de refugiados de 2015 e 2016. Para Sousa (2023b, p. 136), a "diferente reação da UE a estas crises evidencia um duplo *standard* europeu no tratamento das pessoas que fogem da guerra e da violência e têm direito a procurar proteção nos Estados-Membros", sugerindo que este "episódio isolado de humanismo europeu" estará relacionado com razões étnicas e religiosas, tendo em conta que o afluxo

---

40 CEPOL, EIGE, EMCDDA, EUAA, eu-LISA, Eurojust, Europol, FRA e Frontex.

41 CEPOL – *European Union Agency for Law Enforcement Training* – Agência da União Europeia para a Formação Policial

42 TOPCOP – *Training and Operational Partnership against Organized Crime*.

43 Frontex – *European Border and Coast Guard Agency* – Agência Europeia da Guarda de Fronteiras e Costeira.

44 EUAA – *European Union Agency for Asylum* – Agência da União Europeia para o Asilo.

de migrantes registado em 2015 e 2016 era originário de países como a Síria e o Afeganistão, ao contrário dos deslocados ucranianos, maioritariamente de origem europeia (Sousa, 2023a).

Também Gil (2022b) sustenta a hipótese de que a ativação da DPT foi tardia e seletiva, questionando o facto de a mesma apenas ter sido ativada em consequência do afluxo de deslocados da guerra da Ucrânia, quando a sua ativação já teria sido anteriormente solicitada por Itália e por Malta, em 2015, tendo o CUE considerado que não se encontravam reunidas as condições necessárias para o fazer. Mediante esta recusa, alguns autores concluíram que, se a DPT não foi ativada naquele contexto, então dificilmente seria alguma vez ativada. Uma das autoras que defendeu essa posição foi İneli-Ciğer (2022), na sequência de, em 2020[45], a Comissão Europeia ter ponderado revogar a DPT, por considerar que esta já não se encontrava adaptada à realidade atual dos Estados-Membros. Após a surpreendente ativação da DPT em 2022, a autora conclui que a principal razão para a sua não ativação em situações anteriores prendeu-se exclusivamente com a falta de vontade política para o fazer.

Em favor da decisão tomada em 2022, é importante salientar a singularidade e a magnitude da crise dos deslocados do conflito na Ucrânia. Se durante a totalidade do ano de 2015 tentaram entrar em território europeu mais de um milhão de refugiados, nos primeiros dez dias após a invasão da Ucrânia, o mesmo volume de deslocados já tinha procurado refúgio na UE. Verifica-se, portanto, uma grande diferença no que se refere à escala e à velocidade dos dois movimentos de pessoas, sendo que este contraste justificaria a ativação da DPT, no contexto deste conflito (Abrisketa Uriarte, 2023; İneli-Ciğer 2023). Complementarmente, deve também atender-se ao facto de que esta nova crise de deslocados tem origem na Ucrânia, um país que partilha fronteiras com vários Estados-Membros. Tal facto, releva por um lado na proximidade do conflito ao território da UE, ao contrário do que sucedeu em 2015 (conflitos na Síria e Afeganistão), e impossibilita, por outro lado, a utilização de qualquer mecanismo de "estado-tampão", para travar ou refrear o afluxo de migrantes. Por fim, deve também considerar-se que os cidadãos ucranianos não necessitam de visto válido para entrar nos EM, ao contrário do que sucede com os nacionais dos países de proveniência da maior parte dos deslocados da crise de 2015 e 2016. Tal facto facilitou a entrada dos cidadãos ucranianos no espaço da UE e a materialização do propósito da ativação da DPT (Abrisketa Uriarte, 2023; Gil 2022b).

[45] Comissão Europeia (2020b), p.64.

Atendendo ao exposto, considera-se que, com a ativação da DPT em 2022, a UE procurou dar uma resposta urgente a uma crise de dimensão sem precedentes, utilizando os mecanismos ao seu dispor para garantir a proteção de um volume massivo de deslocados. Neste contexto, a DPT mostrou ser uma ferramenta eficaz para evitar o congestionamento e a sobrecarga dos sistemas nacionais de asilo, face ao aumento súbito do número de migrantes que procuravam entrar em território da UE.

Importa também refletir, ao nível da resposta política da UE, no papel desempenhado pelo Conselho Europeu e pelo CUE. No contexto do Conselho Europeu, analisadas todas as conclusões das reuniões desta Instituição, entre a eclosão do conflito e a presente data[46], constata-se a existência de uma posição unificada e consistente do Conselho Europeu relativamente à Ucrânia, que se concretiza em vários pontos transversais: o apoio à soberania e integridade territorial da Ucrânia, o compromisso continuado de auxílio à Ucrânia através de ajuda financeira, militar, diplomática e humanitária, e a ênfase dado à reconstrução e integração europeia da Ucrânia. Não obstante a posição coerente patenteada, destaca-se sobretudo a evolução da posição do Conselho Europeu, direcionando as linhas políticas para ações paulatinamente mais concretas no que respeita à responsabilização da Rússia, ao apoio militar prestado, ao uso de ativos congelados para apoio e reconstrução do país e aos caminhos para a adesão à UE, expressando uma gradual materialização das prioridades do Conselho Europeu face ao conflito (Conselho Europeu, 2022a, 2022b, 2022c, 2022d, 2022e, 2022f, 2023a, 2023b, 2023c, 2023d, 2023e, 2024a, 2024b, 2024c, 2024d, 2024e e 2024f).

Paralelamente, considera-se oportuno analisar de igual modo as medidas tomadas durante as várias presidências do CUE desde 2022 até à data. Aquando do início do conflito, a presidência francesa[47] demonstrou um forte compromisso em apoiar a Ucrânia através de várias medidas concretas, incluindo ajuda financeira, militar e humanitária, bem como a imposição de sanções à Rússia e o apoio à candidatura da Ucrânia à UE (Conselho da União Europeia, 2022d). A presidência checa[48] avançou significativamente neste apoio, especialmente no atinente à dimensão militar, estendendo o apoio à Ucrânia através do Fundo

[46] Para este efeito foram analisadas as conclusões das reuniões ordinárias e extraordinárias do CE decorridas entre 22 de fevereiro de 2022 e 19 de dezembro de 2024.
[47] A França assumiu a presidência do CUE entre 01 de janeiro a 30 de junho de 2022.
[48] A Chéquia assumiu a presidência do CUE entre 01 de julho a 31 de dezembro de 2022.

Europeu de Apoio à Paz[49] e do lançamento da Missão de Assistência Militar da UE (EUMAM). Priorizou também o aumento do apoio financeiro para reconstrução pós-guerra e a gestão de refugiados, através de medidas específicas (Conselho da União Europeia, 2022e). Durante o ano de 2023, tanto a Suécia como a Espanha[50] mantiveram o esforço desenvolvido pelas presidências anteriores ao nível do apoio económico e militar, destacando-se o acordo relativo a uma política de migração e asilo mais restrita, negociado pela Suécia, tendo a Espanha definido como prioridade da sua presidência a extensão da DPT (Conselho da União Europeia, 2023b e 2023c). Já no que resulta das presidências belga e húngara[51] destaca-se a continuação do apoio financeiro para recuperação e reconstrução da Ucrânia através do "Mecanismo para a Ucrânia" bem como das políticas iniciadas pelas anteriores presidências (Conselho da União Europeia, 2024c e 2024d). Face ao exposto, se ao nível do Conselho Europeu se verificou uma materialização gradual das prioridades da UE, no quadro do CUE, as medidas tomadas têm vindo a refletir as prioridades dos Estados-Membros que assumiram a presidência durante o respetivo período. Com efeito, tem-se observado a passagem de uma resposta mais enérgica e ativa, logo após a invasão, para, aparentemente, uma postura mais passiva, de exclusiva continuidade das medidas de apoio económico e militar instituídas pelas presidências anteriores. Tal resulta claramente percetível da consulta das comunicações dos resultados obtidos pelas últimas presidências do CUE, observando-se que a enfâse inicialmente dado ao apoio à Ucrânia, tem vindo gradualmente a perder protagonismo nas comunicações realizadas neste contexto.

6. CONCLUSÕES

A invasão da Ucrânia pela Rússia em fevereiro de 2022 desencadeou um dos maiores desafios humanitários e securitários da história da UE. A crise dos deslocados que se seguiu, testou não só a capacidade da UE para responder a fluxos migratórios em larga escala, mas expôs também fragilidades nas políticas de segurança, migração e asilo. A resposta europeia revelou um compromisso sólido no apoio à Ucrânia, tanto no plano político como no securitário, através da ativação

[49] Conselho Europeu (2024g).
[50] A Suécia assumiu a presidência do CUE entre 01 de janeiro a 30 de junho de 2023 e a Espanha entre 01 de julho a 31 de dezembro de 2023.
[51] A Bélgica assumiu a presidência do CUE entre 01 de janeiro a 30 de junho de 2024 e a Hungria entre 01 de julho a 31 de dezembro de 2024.

da DPT e do reforço da cooperação institucional entre os Estados-Membros, não obstante, verificaram-se também assimetrias significativas na distribuição dos refugiados entre os Estados-Membros e na aplicação das políticas de proteção. Adicionalmente, verifica-se que o conflito funcionou como catalisador das reformas estruturais na política migratória da UE, nomeadamente na reforma do SECA, evidenciando um reposicionamento estratégico do bloco europeu.

Metodologicamente, este trabalho de investigação foi suportado numa análise qualitativa e documental, recorrendo a fontes institucionais, normativas e académicas. Foram consultados vários artigos científicos nas áreas da segurança e da migração, conclusões dos Conselho Europeu e das presidências do CUE e outros documentos institucionais, bem como dados estatísticos do ACNUR e Eurostat. Este estudo integra ainda uma análise crítica das respostas institucionais, na tentativa de clarificar as dinâmicas políticas e securitárias resultantes da crise dos deslocados ucranianos.

No que respeita aos objetivos definidos para esta investigação, a mesma permitiu compreender que os reflexos deste conflito para a segurança interna da UE e a resposta a estes desafios se desenvolveram fundamentalmente em três dimensões. A primeira dimensão prende-se com a decisão inédita de ativar a DPT, a qual permitiu a concessão de proteção imediata a milhões de deslocados ucranianos, sem necessidade de passar por um processo de asilo formal. No entanto, verificaram-se assimetrias profundas na aplicação deste processo, que se materializaram na distribuição desigual dos deslocados, levando à sobrecarga de alguns Estados-Membros em detrimento de outros; nas divergências quanto à extensão da proteção temporária aos cidadãos estrangeiros residentes na Ucrânia, implementada apenas por um número restrito de Estados-Membros, nos quais se inclui Portugal; e nos desafios securitários intensificados pelo afluxo massivo de deslocados, concretizados pelo aumento da incidência de certos fenómenos criminais que colocam desafios adicionais à segurança interna da UE.

A segunda dimensão relaciona-se com a resposta coerente e unificada da UE no apoio à Ucrânia, reforçando o compromisso europeu com a soberania e a integridade territorial ucraniana. No entanto, constata-se que as medidas de apoio à Ucrânia têm vindo a ser influenciadas pelas presidências rotativas do CUE. Se inicialmente se verificou uma resposta energética e coordenada (especialmente sob a presidência francesa e checa), paulatinamente tem-se vindo a observar um decréscimo no que respeita à enfâse dada às medidas de apoio à Ucrânia, refletindo, porventura, um menor dinamismo político neste âmbito.

Por fim, a terceira dimensão da resposta da UE reflete-se na revisão da política de migração e asilo. O conflito impulsionou o debate sobre a reforma do SECA, sendo determinante para a adoção do novo pacto para a migração e asilo. A experiência da ativação da DPT evidenciou a necessidade de edificar um sistema mais flexível e cooperativo, mas veio também reforçar uma abordagem securitária e restritiva da política de asilo da UE, com foco na segurança e controlo das fronteiras bem como na resposta às ameaças híbridas.

No que concerne às limitações desta investigação, destaca-se o facto de esta se basear, essencialmente, em fontes documentais institucionais, as quais podem enviesar a visão crítica sobre a implementação das respostas europeias. Além disso, dada a contínua e atual evolução do conflito e das políticas europeias, algumas conclusões poderão necessitar de reavaliação à luz de futuros desenvolvimentos. Para aprofundamento deste tema, sugere-se que futuras investigações explorem o impacto da DPT na integração socioeconómica dos deslocados ucranianos nos Estados-Membros, a eficácia da reforma do SECA na redistribuição de refugiados e no equilíbrio entre segurança e solidariedade nos Estados-Membros, bem como os efeitos do prolongamento do conflito na resiliência das políticas europeias de segurança e defesa.

A guerra na Ucrânia representa um marco na história da UE, não só pela magnitude da crise humanitária provocada, mas também pelo impacto estrutural nas políticas de segurança e migração. A resposta europeia revelou capacidade de adaptação e solidariedade, contudo, expôs também desafios de implementação e assimetrias na distribuição de responsabilidades entre os Estados-Membros. A longo prazo, a eficácia das políticas adotadas dependerá da manutenção da coesão política e da capacidade da UE em equilibrar solidariedade, segurança e estabilidade institucional.

REFERÊNCIAS BIBLIOGRÁFICAS

Abrisketa Uriarte, J. (2023). The Activation of the Temporary Protection Directive 2001/55/EC for Ukrainian Refugees: A Demonstration of Its Uniqueness. Paix et Securite Internationales - Journal of International Law and International Relations. 11, 1–31. https://doi.org/10.25267/Paix_secur_int.2023.i11.1201

ACNUR – Alto Comissariado das Nações Unidas para os Refugiados. (2024). Refugee Data Finder. https://www.unhcr.org/refugee-statistics/insights/annexes/trends-annexes.html?situation=2.

ACNUR – Alto Comissariado das Nações Unidas para os Refugiados. (2025). Ukraine Refugee Situation. dezembro de 2024. https://data.unhcr.org/en/situations/ukraine.

Berzins, V. (2022). Hybrid warfare: weaponized migration on the eastern border of the EU? The Interdisciplinary *Journal of International Studies: Crisis*. (12) 1. https://doi.org/10.5278/ojs.ijis.v12i1.6992

Bossong, R. (2022). Challenges to internal security and the rule of law from an EU perspective. EU Immigration and Asylum Law and Policy. In *Ukraine's possible EU accession and its consequences*. German Institute for International and Security Affairs (SWP), 07/22/2022 (360 Degrees). https://www.swp-berlin.org/en/publication/ukraines-possible-eu-accession-and-its-consequences#publication-article-67.

Bossong, R. & Rhinard M. (2016). Alternative Perspectives on Internal Security Cooperation in the European Union – Setting the scene. In Bossong, R & Rhinard M. (ed.). *Theorizing Internal Security in the European Union*, 3-27. Oxford University Pres. https://books.google.pt/books?id=ogmDDQAAQBAJ&lpg=RA4-PT7&ots=3B2N7xB0G0&dq=internal%20security%20of%20the%20european%20union&lr&hl=pt-PT&pg=PA1948#v=onepage&q=internal%20security%20of%20the%20european%20union&f=false

Brandão, A. P. (2022). União Europeia e segurança interna coletiva – Progressos e tensões dilemáticas de um ator em construção. In M. F. Monte, F. N. Loureiro & P. J. Morais (Orgs.). *Prevenção, policiamento e segurança: Implicações nos direitos humanos* (pp. 141-158). Escola de Direito da Universidade do Minho. https://repositorium.sdum.uminho.pt/handle/1822/80779

Comissão Europeia. (2015a). Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Agenda Europeia para a Segurança. Comissão Europeia, Bruxelas. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0185

Comissão Europeia. (2015b). Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – Agenda Europeia da Migração. Comissão Europeia, Bruxelas. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52015DC0240

Comissão Europeia. (2016). Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu e ao Conselho – dar cumprimento à Agenda Europeia para a Segurança para combater o terrorismo e abrir caminho à criação de

uma União da Segurança genuína e eficaz. Comissão Europeia, Bruxelas. https://eur-lex.europa.eu/resource.html?uri=cellar:9aeae420-0797-11e6-b713-01aa75ed71a1.0010.02/DOC_1&format=PDF

Comissão Europeia. (2020a). Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – sobre a Estratégia da UE para a União da Segurança. Comissão Europeia, Bruxelas. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52020DC0605

Comissão Europeia. (2020b). Commission staff working document accompanying the document: Proposal for a regulation of the European Parliament and of the Councilon on asylum and migration management and amending Council Directive (EC)2003/109 and the proposed Regulation (EU)XXX/XXX [Asylum and Migration Fund]. Comissão Europeia, Bruxelas. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020SC0207

Comissão Europeia. (2024). Mecanismo de Proteção Civil da UE. https://civil-protection-humanitarian-aid.ec.europa.eu/what/civil-protection/eu-civil-protection-mechanism_pt

Comissão Europeia. (2025). Temporary Reintroduction of Border Control. https://home-affairs.ec.europa.eu/policies/schengen-borders-and-visa/schengen-area/temporary-reintroduction-border-control_en (consultado a 16 de maio de 2025)

Conselho Europeu. (2022a). Reunião extraordinária do Conselho Europeu (24 de fevereiro de 2022) – Conclusões. https://www.consilium.europa.eu/media/54508/st00018-pt22.pdf

Conselho Europeu. (2022b). Reunião do Conselho Europeu (24 e 25 de março de 2022) – Conclusões. https://data.consilium.europa.eu/doc/document/ST-1-2022-INIT/pt/pdf

Conselho Europeu. (2022c). Reunião extraordinária do Conselho Europeu (30 e 31 de maio de 2022) – Conclusões. https://www.consilium.europa.eu/media/56587/2022-05-30-31-euco-conclusions-pt.pdf

Conselho Europeu. (2022d). Reunião do Conselho Europeu (23 e 24 de junho de 2022) – Conclusões. https://www.consilium.europa.eu/media/57465/2022-06-2324-euco-conclusions-pt.pdf

Conselho Europeu. (2022e). Reunião do Conselho Europeu (20 e 21 de outubro de 2022) – Conclusões. https://www.consilium.europa.eu/media/59748/2022-10-2021-euco-conclusions-pt.pdf

Conselho Europeu. (2022f). Reunião do Conselho Europeu (15 de dezembro de 2022) – Conclusões. https://www.consilium.europa.eu/media/60886/2022-12-15-euco-conclusions-pt.pdf

Conselho Europeu. (2023a). Reunião extraordinária do Conselho Europeu (9 de fevereiro de 2023) – Conclusões. https://data.consilium.europa.eu/doc/document/ST-1-2023-INIT/pt/pdf

Conselho Europeu. (2023b). Reunião do Conselho Europeu (23 de março de 2023) – Conclusões. https://data.consilium.europa.eu/doc/document/ST-4-2023-INIT/pt/pdf

Conselho Europeu. (2023c). Reunião do Conselho Europeu (29 e 30 de junho de 2023) – Conclusões. https://data.consilium.europa.eu/doc/document/ST-7-2023-INIT/pt/pdf

Conselho Europeu. (2023d). Reunião do Conselho Europeu (26 e 27 de outubro de 2023) – Conclusões. https://www.consilium.europa.eu/media/67649/20231027-european-council-conclusions-pt.pdf

Conselho Europeu. (2023e). Reunião do Conselho Europeu (14 e 15 de dezembro de 2023) – Conclusões. https://www.consilium.europa.eu/media/68990/europeancouncilconclusions-14-15-12-2023-pt.pdf

Conselho Europeu. (2024a). Reunião extraordinária do Conselho Europeu (1 de fevereiro de 2024) – Conclusões. https://www.consilium.europa.eu/media/69892/20240201-special-euco-conclusions-pt.pdf

Conselho Europeu. (2023b). Reunião do Conselho Europeu (21 e 22 de março de 2024) – Conclusões. https://www.consilium.europa.eu/media/70904/euco-conclusions-2122032024-pt.pdf

Conselho Europeu. (2024c). Reunião extraordinária do Conselho Europeu (17 e 18 de abril de 2024) – Conclusões. https://www.consilium.europa.eu/media/3nblpwkn/euco-conclusions-20240417-18-pt.pdf

Conselho Europeu. (2023d). Reunião do Conselho Europeu (27 de junho de 2024) – Conclusões. https://www.consilium.europa.eu/media/qxqfdhfd/euco-conclusions-27062024-pt.pdf

Conselho Europeu. (2023e). Reunião do Conselho Europeu (17 de outubro de 2024) – Conclusões. https://www.consilium.europa.eu/media/0vvhaodj/20241017-euco-conclusions-pt.pdf

Conselho Europeu. (2023f). Reunião do Conselho Europeu (19 de dezembro de 2024) – Conclusões. https://www.consilium.europa.eu/media/cgpjb53b/euco-conclusions-19122024-pt.pdf

Conselho Europeu. (2024g). Apoio militar da UE à Ucrânia. https://www.consilium.europa.eu/pt/policies/military-support-ukraine/

Conselho Europeu. (2025). Solidariedade da UE com a Ucrânia. https://www.consilium.europa.eu/pt/policies/eu-solidarity-ukraine/#0

Conselho da União Europeia. (2001). Diretiva 2001/55/CE do Conselho de 20 de julho de 2001 relativa a normas mínimas em matéria de concessão de protecção temporária no caso de afluxo maciço de pessoas deslocadas e a medidas tendentes a assegurar uma repartição equilibrada do esforço assumido pelos Estados-Membros ao acolherem estas pessoas e suportarem as consequências decorrentes desse acolhimento. 7 de agosto de 2001. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32001L0055

Conselho da União Europeia. (2009). Estratégia Europeia em Matéria de Segurança: Uma Europa segura num mundo melhor. Serviço das Publicações da União Europeia, Luxemburgo. https://www.consilium.europa.eu/media/30824/qc7809568ptc.pdf

Conselho da União Europeia. (2010). Estratégia de Segurança Interna da União Europeia. Rumo a um Modelo Europeu de Segurança. Serviço das Publicações da União Europeia, Luxemburgo. https://www.consilium.europa.eu/media/30754/qc3010313ptc.pdf

Conselho da União Europeia. (2022a). Decisão de Execução (UE) 2022/382 do Conselho de 4 de março de 2022 que declara a existência de um afluxo maciço de pessoas deslocadas da Ucrânia na aceção do artigo 5. da Diretiva 2001/55/CE, e que tem por efeito aplicar uma proteção temporária. 4 de março de 2022. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022D0382

Conselho da União Europeia. (2022b). Bússola Estratégica para a Segurança e a Defesa – Por uma União Europeia que protege os seus cidadãos, os seus valores e os seus interesses e contribui para a paz e a segurança internacionais. Bruxelas. https://data.consilium.europa.eu/doc/document/ST-7371-2022-INIT/pt/pdf

Conselho da União Europeia. (2022c). Impact of the Russian war of aggression against Ukraine on crime and terrorism in the EU: Follow-up assessment. (7822/22 EXT) 20 de setembro de 2022. https://www.parlament.gv.at/dokument/XXVII/EU/112872/imfname_11178108.pdf

Conselho da União Europeia. (2022d). Results of French Presidency of the Council

of the European Union. https://presidence-francaise.consilium.europa.eu/en/results-of-the-french-presidency-of-the-council-of-the-european-union/

Conselho da União Europeia. (2022e). Results of the Czech Presidency of the Council of the EU. https://czech-presidency.consilium.europa.eu/en/programme/results-of-the-czech-presidency-of-the-council-of-the-eu/

Conselho da União Europeia. (2023a). Refugiados ucranianos: Estados-Membros da UE acordam em prorrogar a proteção temporária. https://www.consilium.europa.eu/pt/press/press-releases/2023/09/28/ukrainian-refugees-eu-member-states-agree-to-extend-temporary-protection/

Conselho da União Europeia. (2023b). Swedish Presidency of the Council of the EU – Results of the Presidency. https://swedish-presidency.consilium.europa.eu/en/programme/results-of-the-presidency/

Conselho da União Europeia. (2023c). Spanish Presidency of the Council of the European Union - The Spanish presidency programme. https://spanish-presidency.consilium.europa.eu/en/programme/the-spanish-presidency-programme/

Conselho da União Europeia. (2024a). Refugiados ucranianos: Conselho prorroga proteção temporária até março de 2026. https://www.consilium.europa.eu/pt/press/press-releases/2024/06/25/ukrainian-refugees-council-extends-temporary-protection-until-march-2026/

Conselho da União Europeia. (2024b). Sanções da UE contra a Rússia. Disponível em: https://www.consilium.europa.eu/pt/policies/sanctions-against-russia/

Conselho da União Europeia. (2023c). Achieving success: highlights of the Belgian presidency. https://belgian-presidency.consilium.europa.eu/en/programme/achieving-success-highlights-of-the-belgian-presidency/

Conselho da União Europeia. (2023d). The Hungarian presidency programme. Disponível em: https://hungarian-presidency.consilium.europa.eu/en/programme/programme/

Dias, V. A. (2022). A crise ucraniana e a transformação das dinâmicas de segurança na europa oriental. Nação e Defesa 162, 45-70. https://www.idn.gov.pt/pt/publicacoes/nacao/Documents/NeD162/Vanda%20Amaro%20Dias.pdf

Dias, V. A. (2023). Um ano de guerra na Ucrânia Como chegámos aqui? Para onde estamos a ir?. Relações Internacionais, 77, 53-61. https://doi.org/10.23906/ri2023.77a06

EU-LISA. (2024). JHA Agencies' contribution to EU solidarity with Ukraine - Joint Paper. Justice and Home Affairs Agencies Network, Bruxelas. https://www.eulisa.europa.eu/sites/default/files/documents/joint-paper-jha-agencies-solidarity-with-ukraine.pdf

European Union External Action. (2022) Russia/Ukraine: Statement delivered by the High Representative Josep Borrell on behalf of the European Union at the extraordinary OSCE Permanent Council. https://www.eeas.europa.eu/eeas/russiaukraine-statement-delivered-high-representative-josep-borrell-behalf-european-union_en

Eurostat. (2025). Beneficiaries of temporary protection at the end of the month by citizenship, age and sex - monthly data. https://ec.europa.eu/eurostat/databrowser/view/migr_asytpsm/default/table?lang=en&category=migr.migr_asy.migr_asytp

Gil, A. R. (2022a). Os Direitos Humanos nos fluxos migratórios "massivos": da crise migratória de 2015 à crise de deslocados da Ucrânia de 2022. C*ompêndio de Direitos Humanos: Comissão dos Direitos Humanos da Ordem de Advogados 2020-2022*, 14-29. https://portal.oa.pt/publicacoes/compendio-de-direitos-humanos-dezembro-2022/sessao-de-lancamento-do-compendio-de-direitos-humanos-cdhoa/

Gil, A. R. (2022b). Proteção internacional revisitada: As soluções da União Europeia para a proteção dos deslocados da Guerra da Ucrânia num contexto de "múltiplas crises de refugiados". *Relações Internacionais*, 75, 45-62. https://doi.org/10.23906/ri2022.75a04

Hermenegildo, R. S. (2017). Uma Matriz Teórica da "Segurança Interna" da União Europeia. *Nação e Defesa*, 146, 106-133. https://revistas.rcaap.pt/nacao/article/view/37540/26260

Hermenegildo, R. S. (2018). A "Segurança Interna" da União Europeia: O caso da guarda costeira e de fronteiras. *Proelium*, VII (14), 147-182. https://run.unl.pt/bitstream/10362/61130/1/A_seguran_a_interna_da_Uni_o_Europeia.pdf

Hermenegildo, R. S. (2024). Implicações da Guerra da Ucrânia na segurança da União Europeia: Incremento da supranacionalização? Relações Internacionais, 83, 29-42. https://doi.org/10.23906/ri2024.83a02

İneli-Ciğer, M. (2022). 5 Reasons Why: Understanding the reasons behind the activation of the Temporary Protection Directive in 2022. EU Immigration and Asylum Law and Policy. https://eumigrationlawblog.eu/5-reasons-why-understanding-the-reasons-behind-the-activation-of-the-temporary-protection-directive-in-2022/

İneli-Ciğer, M. (2023). Reasons for the Activation of the Temporary Protection Directive in 2022: A Tale of Double Standards. In Carreras S. & İneli-Ciğer, M. (ed.). EU Responses to the Large-Scale Refugee Displacement from Ukraine: An Analysis on the Temporary Protection Directive and Its Implications for the Future EU Asylum Policy. (pp. 148-163). European University Institute. https://doi.org/10.2870/90812

Ivančík. R. (2024). On some aspects of European security and defence in the context of war in Ukraine. Security Science Journal, 5 (1). https://www.securityscience.edu.rs/index.php/journal-security-science/article/view/133

Linares, M. A. (2022). La activación y aplicación de la directiva de protección temporal de la Union Europea tras la agresión rusa a Ucrania: logros y desafíos. Anuario de La Facultad de Derecho Universidad de Extremadura (AFDUE), 38, 69–100. https://doi.org/10.17398/2695-7728.38.69

Nagy, B. (2023). About-face or Camouflage? Hungary and the Refugees from Ukraine. In Carreras S. & İneli-Ciğer, M. (ed.). EU Responses to the Large-Scale Refugee Displacement from Ukraine: An Analysis on the Temporary Protection Directive and Its Implications for the Future EU Asylum Policy. (pp.148-163). European University Institute. https://doi.org/10.2870/90812

Parlamento Europeu. (2022). Agressão russa contra a Ucrânia - Resolução do Parlamento Europeu, de 1 de março de 2022, sobre a agressão russa contra a Ucrânia (2022/2564(RSP). Jornal Oficial da União Europeia, C 125, 2-9. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52022IP0052

Parlamento Europeu. (2024). Parlamento valida acordo final do novo pacto sobre migração e asilo da União Europeia. https://www.europarl.europa.eu/news/pt/press-room/20240408IPR20290/parlamento-valida-acordo-final-do-novo-pacto-sobre-migracao-e-asilo-da-ue

Parlamento Europeu e Conselho da União Europeia. (2011). Diretiva 2011/95/UE, de 13 de dezembro de 2011, que estabelece normas relativas às condições a preencher pelos nacionais de países terceiros ou por apátridas para poderem beneficiar de protecção internacional, a um estatuto uniforme

para refugiados ou pessoas elegíveis para protecção subsidiária e ao conteúdo da protecção concedida (reformulação). Jornal Oficial da União Europeia, L 337, 9-26. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:337:0009:0026:pt:PDF

Parlamento Europeu e Conselho da União Europeia. (2013a). Regulamento (UE) n.º 604/2013, de 26 de junho de 2013, que estabelece os critérios e mecanismos de determinação do Estado-Membro responsável pela análise de um pedido de proteção internacional apresentado num dos Estados-Membros por um nacional de um país terceiro ou por um apátrida. Jornal Oficial da União Europeia, L 180, 31-59. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013R0604

Parlamento Europeu e Conselho da União Europeia. (2013b). Diretiva 2013/32/UE, de 26 de junho de 2013, relativa a procedimentos comuns de concessão e retirada do estatuto de proteção internacional (reformulação). Jornal Oficial da União Europeia, L 180, 60-95. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32013L0032

Parlamento Europeu e Conselho da União Europeia. (2013c). Diretiva 2013/33/UE, de 26 de junho de 2013, que estabelece normas em matéria de acolhimento dos requerentes de proteção internacional (reformulação). Jornal Oficial da União Europeia, L 180, 96-116. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:180:0096:0116:PT:PDF

Parlamento Europeu e Conselho da União Europeia. (2016). Regulamento (UE) n.º 2016/399, de 9 de março de 2016, que estabelece o código da União relativo ao regime de passagem de pessoas nas fronteiras (Código das Fronteiras Schengen). Jornal Oficial da União Europeia, L 77, 1-52. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0399

Parlamento Europeu e Conselho da União Europeia. (2024). Regulamento do Parlamento Europeu e do Conselho relativo à gestão do asilo e da migração, que altera os Regulamentos (UE) 2021/1147 e (UE) 2021/1060 e que revoga o Regulamento (UE) n.º 604/2013. Bruxelas, 26 de abril de 2024. https://data.consilium.europa.eu/doc/document/PE-21-2024-INIT/en/pdf

Parusel, B. & Varfolomieieva, V. (2022). The Ukrainian Refugee Situation: Lessons for EU Asylum Policy. Swedish Institute for European Policy Studies. https://www.sieps.se/en/publications/2022/the-ukrainian-refugee-situation-lessons-for-eu-asylum-policy/

Peláez, L. S. (2023). The European Union internal security challenges after the Russian invasion of Ukraine. Security Spectrum: Journal of Advanced Security Research. https://doi.org/10.15158/vemz-1s66

Piçarra, N. (2016). A União Europeia e "a crise migratória e de refugiados sem precedentes": crónica breve de uma ruptura do Sistema Europeu Comum De Asilo. *e-Pública*. (3) 2 (pp. 1-40). https://e-publica.pt/article/34457

Plokhy, S. (2022). A guerra russo-ucraniana: O regresso da história. Editorial Presença.

Reis, L. (2023). A resposta da União Europeia à Guerra da Ucrânia. Relações Internacionais, 77, 35-43. https://doi.org/10.23906/ri2023.77a04

Risch, W. J. (2022). Prelude to War? In Marples. D. R. (ed.). *The War in Ukraine's Donbas: Origins, Contexts, and the Future*. (pp. 7-28). Central European University Press. https://research.ebsco.com/linkprocessor/plink?id=a4f169c8-ea3d-3878-b2f4-36a844c086bd

Sousa, C.U. (2023a). A(s) resposta(s) da União Europeia às crises dos refugiados: Duplo standard europeu? In S.S. Monteiro, C. M. Cebola e E. Lucas (Coords.). *A União Europeia em Tempos de Crise: Direito e Políticas Públicas de 2020 e 2023* (pp. 117-141.). Edições Almedina. https://ijp.upt.pt/wp-content/uploads/2024/01/A-UE-em-tempos-de-crise_compressed.pdf

Sousa, C.U. (2023b). A resposta da União Europeia à "crise" dos refugiados da Ucrânia: Um episódio isolado de humanismo europeu? In L. Tomé, L.V. Pinto e B. Pinto (Coord.). Em torno do *Pensamento de Luís Moita: Humanismo e Relações Internacionais* (pp. 101-114). OBSERVARE - Universidade Autónoma de Lisboa. https://doi.org/10.26619/978-989-9002-28-9.6

Thym, D. (2022). Temporary Protection for Ukrainians: the Unexpected Renaissance of 'Free Choice'. EU Immigration and Asylum Law and Policy. https://eumigrationlawblog.eu/temporary-protection-for-ukrainians-the-unexpected-renaissance-of-free-choice/

Trauner, F & Wolff. S. (2024). The impact of the Russian war against Ukraine on the reform of the common European asylum system. European Politics and Society. https://doi.org/10.1080/23745118.2024.2435401

Vasiliauskienė, V. (2024). The Development of European Union Security Policy. *Public Security & Public Order*, 35, (pp. 334–347). https://doi.org/10.13165/PSPO-24-35-24

Anexo A – Reintrodução temporária do controlo nas fronteiras nos EM (Comissão Europeia, 2025).

EM	NOTIFICAÇÕES DOS EM PARA REINTRODUÇÃO TEMPORÁRIA DE CONTROLO DE FRONTEIRAS INTERNAS ENTRE 2022-2025, JUSTIFICADOS COM A SITUAÇÃO NA UCRÂNIA*																TOTAL PERÍODOS	TOTAL DIAS
Alemanha	12/11/2023 11/05/2024	182	12/05/2024 11/11/2024	184	16/06/2024 15/12/2024	183	16/09/2024 15/03/2025	181	12/11/2024 15/03/2025	124	16/12/2024 15/03/2025	90	16/03/2025 15/09/2025[52]	184			07	1128
Áustria	12/05/2022 11/11/2022	184	12/12/2022 26/12/2022	15	12/05/2023 11/11/2023	184	12/11/2023 11/05/2024	182	12/05/2024 11/11/2024	184	03/06/2024 15/10/2024	166	16/10/2024 15/04/2025	182	12/11/2024 15/05/2025	182	10	1646
	16/04/2025 15/10/2025[53]	183	12/05/2024 11/11/2025[54]	184														
Dinamarca	12/05/2022 11/11/2022	184	12/11/2022 11/05/2023	181	12/05/2023 11/11/2023	184	03/08/2023 10/08/2023	8	11/08/2023 17/08/2023	7	18/08/2023 22/08/2023	5	12/11/2023 11/05/2024	182	12/11/2024 11/05/2025	181	09	1116
	12/05/2025 11/11/2025 [55]	184																
Eslovénia	21/10/2023 30/10/2023	10	31/10/2023 19/11/2023	20	20/11/2023 09/12/2023	20	10/12/2023 21/12/2023	12	22/12/2023 21/06/2024	183	22/06/2024 21/12/2024	183	22/12/2024 21/06/2025[56]	182			07	610
Estónia	03/03/2022 12/03/2022	10	13/03/2022 01/04/2022	20	02/04/2022 21/04/2022	20	22/04/2022 21/05/2022	30	22/05/2022 31/05/2022	10							05	90
França	01/11/2022 30/04/2023	181															01	181

[Cont.]

Itália	19/06/2024 18/12/2024	183															01	183
Noruega	12/11/2022 11/05/2023	181	12/05/2024 11/11/2024	184													02	365
Suécia	12/05/2022 11/11/2022	184															01	184

*Períodos de reintrodução de controlo de fronteiras assinalados a azul encontram-se atualmente a vigorar.

---

52 Fronteiras da Alemanha com a França, Luxemburgo, Bélgica, Países Baixos, Dinamarca, Áustria, Suíça, Chéquia e Polónia.
53 Fronteiras da Áustria com a Eslováquia e Chéquia.
54 Fronteiras da Áustria com a Hungria e Eslovénia.
55 Fronteiras da Dinamarca com a Alemanha.
56 Fronteiras da Eslovénia com a Croácia e Hungria.

ESTUDO 4 – A SEGURANÇA INTERNA NA QUARTA REVOLUÇÃO INDUSTRIAL: OPORTUNIDADES E DESAFIOS

INTERNAL SECURITY IN THE FOURTH INDUSTRIAL REVOLUTION: OPPORTUNITIES AND CHALLENGES

André Filipe Lopes Barreira
Capitão GNR

RESUMO

O presente artigo tem por objeto de estudo a influência da Quarta Revolução Industrial na Segurança Interna, impulsionada pelas tecnologias emergentes que representam novas oportunidades e desafios para as forças de segurança.

A metodologia adotada assenta numa abordagem qualitativa, sustentada em análise bibliográfica, identificando-se oportunidades associadas à modernização das práticas policiais através da automação de processos, avaliações dinâmicas de risco e análise preditiva de dados em tempo real. Em paralelo identificam-se desafios impostos pelas crescentes ciberameaças, bem como, dilemas legais e éticos associados à vigilância massiva e ao potencial de discriminação dos algoritmos.

Esta investigação conclui que a segurança interna se confronta com um novo paradigma operativo, no qual as tecnologias emergentes oferecem diversas oportunidades a serem exploradas para melhorar a eficácia e eficiência das operações. Contudo, existem limitações que devem ser consideradas, como sejam a falta de consenso quanto à sua eficácia, a incapacidade analítica, assim como, dilemas éticos e legais na utilização de algoritmos que exigem, não só uma adaptação do quadro legal, como também, uma integração coordenada destas soluções tecnológicas nas mudanças organizacionais, sendo essencial uma abordagem crítica e responsável à sua implementação.

Palavras-chave: Quarta Revolução Industrial, Segurança Interna, Tecnologias Emergentes, Análise Preditiva, Ciberameaças

ABSTRACT

The purpose of this article is to study the influence of the Fourth Industrial Revolution on Homeland Security, driven by emerging technologies that represent new opportunities and challenges for security forces.

The methodology adopted is based on a qualitative approach, supported by bibliographic analysis, identifying opportunities associated with the modernisation of police practices through process automation, dynamic risk assessments and predictive data analysis in real time. At the

same time, challenges posed by growing cyberthreats are identified, as well as legal and ethical dilemmas associated with mass surveillance and the potential for algorithmic discrimination. This research concludes that internal security is facing a new operational paradigm, in which emerging technologies offer various opportunities to be exploited to improve the effectiveness and efficiency of operations. However, there are limitations that must be considered, such as the lack of consensus on their effectiveness, analytical incapacity, as well as ethical and legal dilemmas in the use of algorithms that require not only an adaptation of the legal framework, but also a coordinated integration of these technological solutions into organisational changes, and a critical and responsible approach to their implementation is essential.

***Keywords**: Fourth Industrial Revolution, Internal Security, Emerging Technologies, Predictive Analytics, Cyberthreats*

1. INTRODUÇÃO

A Quarta Revolução Industrial (4RI) representa uma transformação profunda na história da humanidade que está a ser impulsionada por avanços tecnológicos que vão redefinir a forma como vivemos, trabalhamos e nos relacionamos. No contexto da segurança interna, estas mudanças trazem consigo tanto oportunidades, quanto desafios que necessitam de uma análise cuidadosa e interdisciplinar.

Assim, o objetivo central desta investigação é identificar quais as principais oportunidades e desafios para a segurança interna decorrentes da 4RI em curso, justificando-se este estudo pela necessidade de compreender como a segurança interna pode beneficiar na utilização destas tecnologias e que desafios deve acautelar neste processo.

Esta investigação baseou-se numa análise bibliográfica de fontes primárias e secundárias, com um enfoque teórico-analítico e institucional, tendo sido referenciadas obras de destaque, incluindo revisões sistemáticas, para fundamentar de forma robusta o impacto real da 4RI na segurança interna e explorar as suas implicações.

O estudo está organizado em três partes principais. Inicialmente apresentam-se de forma sumária os conceitos estruturais de segurança interna e da 4RI. Na segunda parte são exploradas as oportunidades de transformação proporcionadas pelas tecnologias emergentes, destacando-se a integração da inteligência artificial na tomada de decisões e a análise preditiva. Na terceira parte são discutidos os desafios na utilização destas tecnologias e respetivas implicações éticas e legais, e por fim, apresentam-se as considerações finais e recomendações do trabalho.

2. A SEGURANÇA INTERNA E O ADVENTO DA QUARTA REVOLUÇÃO INDUSTRIAL

Cristina Sarmento defende que o conceito de segurança interna depende das conceções de Estado, indicando que "a segurança está na base fundamental histórica do Estado. A emergência histórica do Estado moderno, desde Maquiavel, depende da capacidade do poder de assegurar a segurança, numa simbiótica relação com o espaço, com a sua delimitação física e com a capacidade de manter a ordem fundada na legitimidade do poder, sobre o conjunto dos indivíduos que habitam esse espaço" (Sarmento, 2009, p.16).

A mesma conclui que o estudo da segurança interna deverá ser interdisciplinar uma vez que abrange não só dimensões policiais e políticas, mas também tecnológicas, económicas, culturais, entre outras, pelo que se iniciará por apresentar neste estudo os conceitos enquadradores da segurança interna e da 4RI, para posteriormente se poderem inferir relações entre ambos, bem como oportunidades e desafios.

2.1. A segurança interna

A Constituição da República Portuguesa (CRP) é a base normativa da qual decorre a delimitação do conceito de segurança interna no enquadramento jurídico português, consagrando logo no seu art.º n.º 27.º/1 o Direito à Segurança e indicando-nos que cabe à Polícia defender a legalidade democrática, garantir a segurança interna e os direitos dos cidadãos nos termos do seu art.º 272.º/1.

Pese embora a referência expressa no texto constitucional, o conceito de segurança interna encontra a sua definição na atual Lei de Segurança Interna através da Lei n.º 53/2008 de 29 de Agosto, na qual é definida no n.º 1 do art.º 1.º como a atividade 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.

Este conceito extravasa os três domínios tradicionais de atuação da segurança interna elencados por Gouveia (2020), nomeadamente a manutenção da ordem pública, a prevenção e repressão criminal e a por fim a investigação criminal, essencialmente pelas mudanças que ocorreram na sociedade e necessidades para fazer face a novas ameaças emergentes.

Em termos europeus, e de acordo com a Estratégia de Segurança Interna da União Europeia (UE), o conceito de Segurança Interna estende-se a múltiplos setores, com o objetivo de fazer face a ameaças graves e a outras que tenham um impacto direto na vida, na segurança e no bem-estar dos cidadãos, abrangendo não apenas a segurança face a atos criminosos, mas também face a catástrofes naturais e provocadas pelo homem (Conselho da UE, 2010).

Importa nesta investigação destacar que a UE reconhece o impacto da era digital[57], decorrente, por exemplo, do aumento da interdependência que existe de infraestruturas digitais (Comissão Europeia, 2020), e reitera como uma das principais ameaças à segurança interna a cibercriminalidade, a qual tem merecido especial atenção por diversas estruturas Europeias e nomeadamente pela Europol[58] (Europol, 2024).

2.2. A QUARTA REVOLUÇÃO INDUSTRIAL

Uma nova onda de avanços tecnológicos tem levado gradualmente a humanidade a uma nova era de globalização, apelidada no *World Economic Forum* em 2016 de 'Quarta Resolução Industrial'.

Este conceito representa uma transformação profunda na história da humanidade, caracterizada pela convergência das esferas física, digital e biológica, indicando Klaus Schwab que "*as mudanças são tão profundas que, na perspetiva da história da humanidade, nunca houve um tempo de maior promessa ou perigo potencial*" (2016, p. 8).

Pese embora a 4RI seja frequentemente associada ao conceito de "Indústria 4.0", que se foca na digitalização e automação dos sistemas de produção, segundo a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) vai muito além disso, abrangendo impactos económicos, políticos e sociais mais amplos (OCDE, 2017).

Este fenómeno assenta na convergência de tecnologias como a IA, a Robótica Avançada, a *Internet of Things* (IoT), a *Big Data*, a Biotecnologia entre

---

[57] Neste particular foi criado o *European Cybercrime Centre* (EC3) para fortalecer a resposta das autoridades policiais ao cibercrime, incluindo fraudes online, exploração sexual infantil e crimes na *dark web*.

[58] As prioridades da Europol são guiadas pelo *Serious and Organised Crime Threat Assessment*, que avalia as ameaças do crime organizado na Europa e essas prioridades determinam o trabalho operacional no âmbito do *European Multidisciplinary Platform Against Criminal Threats*, uma plataforma que promove a cooperação entre os Estados-Membros, a Europol e outros parceiros.

outros sistemas ciber-físicos que se distinguem das revoluções anteriores pela velocidade e amplitude das mudanças que se perspetivam a curto prazo, não se limitando apenas à automação de processos, mas engloba a criação de ecossistemas inteligentes onde máquinas, sistemas e humanos interagem de forma colaborativa, influenciando por conseguinte a forma como os seres humanos vivem, trabalham e se relacionam (Beier et al., 2020).

Ou seja, a 4RI não se limitará à mera criação de novas máquinas e processos inteligentes, abrangendo na sua essência, mudanças profundas na forma como o valor económico, político e social é criado, trocado e distribuído, que influenciará a vida quotidiana das pessoas, das empresas e das estruturas de governação (Cetrulo & Nuvolari, 2019; Lee, Malerba & Primi, 2021), o que naturalmente irá impactar as próprias dinâmicas de funcionamento das forças policiais em si e da segurança interna como um todo.

Por outro lado, tem sido defendido desde a conceptualização inicial que a 4RI aumentará a qualidade de vida a nível global (Schwab, 2016), no entanto as tendências tecnológicas emergentes poderão expor a humanidade a novas ameaças, riscos e desafios de segurança que importa antecipadamente perspetivar pois a 4RI irá trazer grandes implicações económicas, sociais e políticas a médio prazo, que terão consequências no emprego, distribuição de riqueza, no bem-estar e no meio ambiente (Müller, Kiel & Voigt, 2018).

A própria UE já vem há alguns anos a relevar o papel das tecnologias emergentes e em específico da IA para melhoria da eficácia do trabalho policial, como é exemplo a análise de grandes volumes de dados e identificação de padrões criminais, nomeadamente através deteção de conteúdos terroristas online (Comissão Europeia, 2020).

3. OPORTUNIDADES DE TRANSFORMAÇÃO

Como detalhado anteriormente a 4RI está a transformar significativamente a forma como as organizações trabalham, processam informação e tomam decisões, existindo a expectativa que estas tecnologias emergentes tornem o modelo policial mais eficaz, comparativamente ao modelo tradicional implementado, pelo que importará aferir por um lado as possibilidade abertas pela 4RI mas também a sua eficácia para avaliar a sua admissibilidade pois se os sistemas não forem eficazes estão condenados logo à partida.

3.1. Modernização e integração da IA na tomada de decisões

A convergência da IoT e da IA (AIoT) pode vir a transformar as políticas públicas de segurança, tornando as práticas tradicionais de segurança mais proativas e eficientes, através da automação de processos e da análise preditiva de dados em tempo real (Huang, Chou & Wu, 2021). Assim, as organizações policiais podem aumentar a eficiência e a rapidez das respostas em situações críticas, por exemplo com a utilização de sensores, *edge computing* e IA que possibilitará a deteção automática de eventos críticos, como ocorrência de disparos num determinado local ou de movimentos suspeitos numa zona de interesse e a consequente emissão de alertas imediatos para as patrulhas às ocorrências (Huang et al., 2021).

Por outro lado, o rápido crescimento e disponibilização, ao grande público destas tecnologias emergentes, pode ter também impacto contra a segurança de um país, produzindo novas formas de crime[59], novos *modi operandi* e alvos destas práticas criminais (Choo, Smith & McCuster, 2007).

Esta realidade está a fazer com que as próprias autoridades policiais tenham que se adaptar a estes novos problemas de segurança e formas emergentes de crime (Loveday, 2017). Em termos europeus, Ernst *et al*. (2021) dá como exemplo o ano de 2016 onde só a Polícia Nacional dos Países Baixos estava a realizar 130 projetos tecnológicos[60].

Relativamente às possibilidades de integração de dados na tomada de decisão, importa relevar a revisão sistemática a 192 artigos[61] elaborada por Afzal e Panagiotopoulos (2024), na qual detalharam a forma como os dados estão a transformar as práticas policiais e as próprias organizações, pretendendo identificar os efeitos do uso de dados em áreas como tomada de decisão automatizada e analisar as implicações para a transformação organizacional e a evolução das estratégias de policiamento.

---

[59] Neste particular, Kaspersen (2015) enfatiza as implicações de tecnologias emergentes, como drones, IA, nanotecnologia e impressão 3D, na segurança, uma vez que podem ser usadas por atores não estatais em atividades criminosas e espionagem, alertando para os riscos de proliferação considerando a facilidade de copiar tecnologias críticas e consequentemente contornar os sistemas de fiscalização tradicionais.

[60] A nível nacional podemos também verificar um conjunto alargado de projetos tecnológicos relacionados com a 4RI, em entidades policiais como é o caso da PJ (https://www.policiajudiciaria.pt/projetos-financiados/).

[61] A maioria dos estudos são qualitativos (n=128) e baseados em estudos de caso, maioritariamente nos EUA, seguido do Reino Unido, Europa, Canadá, Austrália, Ásia e África.

Inicialmente foram identificados três tipos de dados passíveis de análise e integração, nomeadamente, dados direcionados[62], dados automatizados[63] e dados de fontes abertas[64] (Afzal & Panagiotopoulos, 2024).

Com este tipo de dados, Afzal e Panagiotopoulos (2024) concluíram que podem ser construídos quatro tipos de processos orientados por dados: a construção do crime onde se podem utilizar dados direcionados para visualizar proativamente aglomerados de crimes e comportamento criminal, priorizar alvos e realocar recursos para prevenção, identificar *hotspots* e potenciais infratores, identificar abordagens ambientais e por fim determinar a aplicação da lei e alcance comunitário da intervenção.

Na deteção do crime, podem ser recolhidos de forma proativa informações para extrair indicadores físicos e sociais, criando perfis de sinalização de eventos criminais e desordem.

Na automação da vigilância, podem ser aplicadas técnicas de análise e extração de informações de sensores e dispositivos eletrónicos para detetar padrões e atividades suspeitas em áreas de interesse.

E por fim, na automação da desordem, onde podem ser combinadas mineração de dados e aprendizagem automatizada, para avaliar tensões comunitárias e identificar atores envolvidos em distúrbios sociais, utilizar análise de processamento de linguagem para categorizar sentimentos em redes sociais e identificar padrões de discurso de ódio.

Contudo, pese embora as forças policiais acumulem vastas quantidades de dados digitais, frequentemente carecem da capacidade tecnológica para os analisar de forma rápida e precisa, de modo a tirar o máximo proveito das informações que eles podem oferecer (Babuta *et al.*, 2018), pelo que existe a necessidade de se desenvolverem novas formas mais eficazes de gestão de dados, recorrendo a ferramentas analíticas para identificar padrões, prever riscos futuros e direcionar

---

62 Pertencem às próprias forças policiais ou organizações estatais, tais como registos de crimes, relatórios de acidentes, perfis de infratores, chamadas de serviço, informações comunitárias, mandados, padrões de tráfego, chamadas de emergência, entre outros

63 Recolhidos por sensores e dispositivos eletrónicos, nos quais se incluem CCTV, câmaras corporais, leitores automáticos de matrículas, sensores ambientais, smartphones, entre outros.

64 São obtidos através de dispositivos, plataformas ou sistemas de código aberto, principalmente de redes sociais como *Facebook* ou *YouTube*.

os recursos de maneira mais eficiente[65] (Brayne, 2017).

Neste contexto, Babuta *et al.* (2018) indicam que a tecnologia de machine learning apresenta-se como uma solução promissora, podendo ser usada em ferramentas de policiamento preditivo, algoritmos para avaliação de risco de infratores[66], planos de gestão de risco de reincidência[67], ou até para otimização de recursos, como o algoritmo usado pela Polícia de Norfolk para avaliar a "solvabilidade" de casos de roubo, com o objetivo de informar decisões de priorização sobre que casos devem ser encaminhados para investigação, permitindo que as forças policiais se concentrem em casos com maior probabilidade de serem resolvidos.

Porém, para além desta capacidade, e para que exista um aproveitamento por parte das instituições policiais destas tecnologias e processos de inovação é necessário, segundo Ernst et al. (2021), cinco requisitos essenciais: o desenvolvimento da ideia, as pessoas envolvidas, as transações entre os envolvidos, a influência do contexto e os resultados do processo.

Na sua investigação longitudinal junto da polícia holandesa, cujo objetivo foi identificar os fatores que promovem ou inibem a inovação tecnológica desde a conceção até a implementação[68], Ernst *et al.* (2021) concluíram que a inovação tecnológica depende mais de fatores sociais e organizacionais do que da própria tecnologia em si.

Ou seja, fatores como as características das pessoas envolvidas (motivação e perseverança), a colaboração dentro e fora da organização policial e a capacidade de adaptação às mudanças foram apontados como promotores da inovação, e por outro lado, em oposição, fatores como a falta de capacidade, continuidade e qualidade dos recursos humanos, a falta de uma visão estratégica sobre tecnologia

---

[65] Para além deste aspeto Brayne (2017) vai mais longe e indica que a integração de dados de diferentes instituições pode facilitar uma abordagem mais holística da segurança e não só aumentar a eficácia das operações de segurança, mas também promover uma melhor coordenação entre diferentes agências governamentais, pois a fusão de sistemas de dados anteriormente separados, permite que a polícia utilize informações recolhidas em contextos não criminais, como dados de saúde e serviços sociais, para melhorar a vigilância e a gestão de riscos.

[66] À semelhança do *Assessment Risk Tool* da polícia de Durham, no Reino Unido, que utiliza *random forest forecasting* para classificar indivíduos em termos de risco de cometerem um crime violento (Babuta *et al.*, 2018).

[67] Como a ferramenta *Offender Assessment System* utilizada em Inglaterra e no País de Gales (Babuta *et al.*, 2018.

[68] Nesta investigação foram analisados longitudinalmente 13 projetos de inovação tecnológica entre janeiro de 2017 e fevereiro de 2018 (Ernst *et al.*, 2021).

e liderança desenquadrada, são identificados como inibidores, referindo os autores que a tecnologia por si só não garante o sucesso da inovação, sendo necessário um alinhamento com mudanças organizacionais.

3.2. *Big data* e análise preditiva

Como vimos no ponto anterior uma das tecnologias emergentes da 4RI com maior expectativa para alcançar resultados na área da segurança interna é a *big data* e análise preditiva, e nesta área relevamos, pela sua importância, a revisão sistemática de Lee, Bradford e Posch (2024) – "*The Effectiveness of Big Data-Driven Predictive Policing: Systematic Review*", onde se procura avaliar a eficácia do policiamento preditivo impulsionado por *big data* em 161 artigos científicos dessa área.

Na delimitação do conceito de policiamento preditivo, assume-se que o mesmo pode ser definido como "aplicação de técnicas analíticas – particularmente técnicas quantitativas – para identificar alvos para intervenção policial e prevenir crimes ou resolver crimes passados através de previsões estatísticas" (Perry, 2013, p. 1).

Lee *et al*. (2024) fazem uma diferenciação entre policiamento preditivo baseado em 'pessoas' e policiamento preditivo baseado em 'locais', sendo o primeiro associado a reincidência de comportamentos criminais com base em registos policiais e nas características dos infratores, e o segundo baseado na alocação de recursos policiais com base na análise preditiva da distribuição espacial e temporal do crime, semelhante ao utilizado no policiamento em '*hotspots*', onde inclusive já existe um corpo teórico que tende a comprovar a sua eficácia na redução da criminalidade conforme apontado na revisão sistemática de Braga, Papachristos e Hureau (2012).

O foco de Lee et al. (2024) foi na segunda categoria por considerar ser aquele que é mais viável de analisar e onde o contexto policial pode efetivamente produzir resultados[69].

Meijer e Wessels (2019), indicam que, embora existam alegações de que o policiamento preditivo pode reduzir a criminalidade e melhorar a eficiência policial, as evidências empíricas são mistas, pois alguns estudos mais recentes reportaram

[69] Contrariamente ao policiamento preditivo baseado em 'pessoas' que envolve uma forte componente associada à fase de monitorização da detenção em estabelecimento prisional ou liberdade condicional, sendo consequentemente mais intrusivo e controverso do ponto de vista ético (Dressel e Farid, 2018; Lee et al., 2024).

resultados positivos no policiamento preditivo, nomeadamente na redução de crimes (Carter *et al*., 2021), outros houve que tiveram resultados contraditórios, dependendo da tipologia criminal ou dos métodos de intervenção utilizados (Ratcliffe *et al*., 2021; Vomfell, Hardle & Lessmann, 2018), pelo que importa perceber a sua real eficácia.

Para tal, Lee *et al*. (2024) analisaram e classificaram os 161 estudos científicos[70] em quatro tipos, com base na força da evidência que apresentavam[71], tendo verificado que apenas 3.7% dos estudos (n=6) relataram testes de algoritmos preditivos em aplicações policiais reais (3 estudos do tipo 1 e 3 estudos do tipo 2), sendo que a maioria dos estudos retrospetivos (n=134) foi do tipo 3, ou seja, estudos que construíram um modelo de previsão direto baseado em algoritmos.

Entre os testes do tipo 1, relevamos o de Braga e Bond (2008) que usou dados de chamadas para o serviço de emergência e dados qualitativos para prever *hot spots* de crime e aplicar intervenções policiais direcionadas, encontrando uma redução de 19,8% na criminalidade geral, o estudo de Carter et al. (2021) que teve efeitos significativos na redução do "dano social" em hotspots associados a locais de overdose de drogas e por fim Ratcliffe *et al*. (2021) onde foi testado um modelo preditivo usando dados de crime, demográficos e de censo, tendo encontrado uma redução de 31% nos crimes contra a propriedade quando aplicado com viaturas policiais referenciadas no estudo.

Quanto as estudos do tipo 2, destacam-se o de Wyatt e Alexander (2010) relacionado com a implementação de policiamento visível em locais com altos índices de acidentes de trânsito em Nashville (EUA), tendo reportado uma redução nos acidentes fatais (15.9%) e ferimentos (30.8%), contudo sem grupo de controlo que impossibilita comparações, e outros dois estudos, Florence *et al*. (2011) que obteve resultados mistos e Hunt, Saunders e Hollywood (2014) com resultados não significativos, sugerindo que a implementação falhou devido a problemas organizacionais e de fidelidade ao programa.

---

[70] Relativamente ao contexto das investigações importa relevar que a grande maioria dos estudos se reporta aos EUA (n=101), seguido pela China (n=11), Canadá (n=9), Reino Unido (n=8) e Brasil (n=5).

[71] Nomeadamente categorizando de Tipo 1: Estudos com aplicação no mundo real que testaram efeitos de deslocamento do crime; Tipo 2: Estudos com aplicação no mundo real que não testaram efeitos de deslocamento; Tipo 3: Estudos retrospetivos que testaram a precisão de algoritmos preditivos com base em dados passados.; Tipo 4: Estudos retrospetivos que identificaram variáveis preditoras de crime, sem construir um modelo preditivo completo (Lee et al., 2024),

Quanto aos restantes estudos, a maioria (130) relatou resultados otimizados ou favoráveis, sugerindo que os seus algoritmos eram eficazes na previsão do crime, no entanto, Lee *et al.* (2024) indicam que a grande maioria desses estudos com resultados positivos pode refletir um viés de publicação.

Em suma, de acordo com a investigação de Lee *et al.* (2024) conclui-se que a eficácia do policiamento preditivo ainda não está comprovada, devido ao reduzido número de estudos com aplicações no mundo real e à grande quantidade de estudos retrospetivos com possíveis vieses de publicação, pois apesar de muitos apresentarem resultados otimizados, isso não prova a eficácia do policiamento preditivo no mundo real, uma vez que a previsão algorítmica é apenas um primeiro passo, sendo necessário testar os modelos de uma forma mais rigorosa no terreno, com grupos de controlo e tratamento, bem como de intervenções bem definidas e avaliações de possíveis efeitos de deslocamento e vieses algorítmicos.

4. DESAFIOS EMERGENTES

Esta transformação tecnológica traz desafios que exigem uma abordagem interdisciplinar e que impõem uma análise crítica, especialmente no que concerne à ética, dependência tecnológica e formação de recursos humanos que será necessária para acautelar se as instituições procurarem implementar estas tecnologias emergentes.

4.1. Cibersegurança e ciberameaças

Um dos primeiros aspetos a considerar na utilização destas tecnologias é precisamente as ameaças iminentemente digitais que terão de ser consideradas. Para tal, importa perceber que o conceito de cibersegurança abrange "todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas" cfr. art.º 2.º ponto 1, do Regulamento (UE) 2019/881, de 17 de abril de 2019.

Das várias ameaças a considerar, o mais recente relatório da European Union Agency for Cybersecurity (ENISA) indica que a IA, IoT e computação em nuvem trazem desafios significativos, destacando a manipulação de dados[72] (incluindo

[72] Estes ataques visam comprometer a precisão dos sistemas de IA, manipulando dados de treino ou inferência, o que pode levar a decisões erradas e à perda de confiança nos sistemas (ENISA, 2024).

ataques de *data poisoning* e *adversarial attacks*), especialmente com a adoção generalizada de modelos de *machine learning* e IA. Além disso, a proliferação de dispositivos IoT e a dependência de infraestruturas em nuvem aumentam a superfície de ataque, expondo organizações a vulnerabilidades como violações de dados e *ransomware* (ENISA, 2024).

Outro aspeto a considerar é a integração de IA generativa e *deepfakes* que introduz riscos significativos, como a criação de campanhas de *phishing* altamente personalizadas e a manipulação de informações para influenciar a opinião pública[73] (ENISA, 2024).

Sobre o impacto destas ciberameaças, Cremer et al. (2022) estimam que tenha custado à economia global cerca de 1 trilião de dólares em 2020, o que representa um aumento de mais de 50% relativamente a 2018. Os autores realizaram uma revisão sistemática da literatura existente sobre cibersegurança e gestão de ciberiscos, analisando 5219 estudos revistos por pares e enfatizaram a necessidade de melhorar as medidas de cibersegurança, especialmente em setores críticos como infraestruturas energéticas e de saúde, que são frequentemente alvo de ciberataques (Cremer et al., 2022).

Por outro lado, Cremer et al. (2022) indicam que a falta de transparência e a relutância das organizações em divulgar incidentes de cibersegurança agravam a escassez de dados, sendo estes essenciais para a avaliação precisa dos riscos e a formulação de políticas eficazes de cibersegurança e indicam também como necessidade premente a criação de um sistema de relatórios obrigatórios sobre ciberincidentes que poderia melhorar a compreensão e a consciencialização sobre esses mesmos riscos.

A Europol partilha parte destas preocupações, enfatizando que a rápida evolução tecnológica tem proporcionado novas ferramentas e métodos para cibercriminosos, que se adaptam com agilidade para explorar vulnerabilidades no espaço digital. O *Internet Organised Crime Threat Assessment* (IOCTA) refere que a IA surge agora como um dos principais catalisadores desta transformação sendo utilizada tanto para aperfeiçoar ataques já existentes como para criar novas

[73] Relacionado com este ponto, verificam-se ataques de *vishing* e *smishing*, que utilizam IA para gerar áudio e texto ainda mais convincentes e sofisticados, dificultando a deteção e prevenção (ENISA, 2024).

formas de criminalidade[74], sendo que a *dark web* e plataformas de comunicação encriptadas são os principais canais onde se comercializam ferramentas e serviços para ciberataques, incluindo *large language models* (LLMs) maliciosos e serviços de *phishing* (Europol, 2024).

Este 'modelo de negócio criminal' permite que indivíduos com pouca experiência técnica se envolvam em atividades criminosas, intensificando o volume e a diversidade das ameaças, sendo indicado por exemplo que os ataques de ransomware têm-se tornado mais frequentes, com os criminosos a visar cada vez mais pequenas e médias empresas, com modelos de extorsão que incluem furto, divulgação de dados e encriptação de sistemas.

Por fim, importa refletir que a Europol, à semelhança de qualquer força policial opera sistemas complexos, como o *Secure Information Exchange Network Application* e o *Europol Information System*, que são essenciais para a partilha de informações entre Estados-Membros, no entanto, a dependência destes sistemas pode tornar a agência e os seus parceiros mais vulneráveis a ciberataques, que podem comprometer a segurança das informações e a eficácia das operações policiais, sendo imperativo que se invista em medidas de cibersegurança robustas, como por exemplo a implementação de medidas como a autenticação multifatorial e a monitorização contínua de ameaças, bem como o investimento em sistemas redundantes para garantir a resiliência das suas infraestruturas tecnológicas (ENISA, 2024; Europol, 2024).

Perante a complexidade deste cenário digital que apresentamos e a rápida evolução das técnicas criminosas, a cibersegurança enfrenta desafios multifacetados que exigem uma constante adaptação das estratégias de defesa e investigação e uma maior colaboração entre as autoridades policiais, o setor privado e a comunidade internacional.

4.2. Privacidade e vigilância

Relativamente à análise preditiva e à vigilância automatizada, embora ofereçam, como vimos anteriormente, oportunidades para melhorar a prevenção de crimes e respetiva eficiência operacional, vários autores têm sido consensuais nas

[74] Por exemplo, os LLM são utilizados para gerar *phishing* nas burlas online de forma automatizada, tornando o ataque mais convincente, *deepfakes* são utilizados em fraudes de identidade e extorsão (Europol, 2024).

preocupações relativamente à vigilância massiva e ao potencial de discriminação dos algoritmos (Brayne & Christin, 2020; Afzal & Panagiotopoulos, 2024; Lee et al., 2024; Fortes et al., 2022; Gandhi, 2024).

Entre os vários exemplos destas práticas importa destacar situações reais nos quais foram apontadas más práticas, nomeadamente utilização de sistemas de reconhecimento facial em operações policiais que levaram a disparidades raciais em detenções conforme apontado por Johnson et al. (2022), o uso das *Strategic Subjects List* de Chicago, um sistema para prever a propensão à violência que foi criticado por "*racial profiling*" (Saunders *et al.*, 2016), ou o *Harm Assessment Risk Tool*, usado pela polícia de Durham na Inglaterra, que pode perpetuar vieses, pois não considera fatores como as circunstâncias familiares ou a importância do trabalho dos visados (Oswald et al., 2018).

Um dos estudos de caso a nível europeu sobre este desafio da 'privacidade vs. vigilância' é precisamente na agência Frontex, estudada por Gandhi (2024) que é caracterizada como 'hub de vigilância e partilha de dados', considerando a utilização de tecnologias avançadas, como drones, sistemas de vigilância por satélite, e algoritmos de análise de risco, ambas tecnologias emergentes da 4RI.

Neste particular é destacado o mandato cada vez mais amplo de missões da Frontex ao longo dos anos, que inclui agora a gestão de sistemas de informação avançados, como o *European Travel Information and Authorisation System* (ETIAS) e o *European Border Surveillance System*, sendo argumentado por Gandhi (2024) que esta expansão não foi acompanhada por salvaguardas adequadas para proteger os direitos fundamentais, como a privacidade e a proteção de dados, especificando que o sistema ETIAS pode representar uma ameaça significativa aos direitos fundamentais, uma vez que se baseia em avaliações de risco automatizadas que podem levar a discriminação e falsos positivos, considerando a falta de transparência no funcionamento dos algoritmos e a ausência de uma avaliação de impacto sobre os direitos fundamentais.

Em concreto, o ETIAS irá utilizar[75] algoritmos para avaliar o risco de viajantes de países terceiros e consequentemente tomada de decisão automatizada, tendo sido alegado que embora os algoritmos tenham o poder de influenciar o estatuto legal de cidadãos de países terceiros, não o devem determinar por si só,

[75] O sistema já sofreu desde 2020 diversos atrasos para entrada em funcionamento, sendo expectável a sua entrada em 2025 (https://etias.com/etias-launch-pushed-to-2025).

pelo que a intervenção humana terá sempre que se manter como um elemento crucial no processo de tomada de decisão, sendo igualmente determinante garantir que os sistemas de tomada de decisão automatizada sejam justos, transparentes e responsáveis, de modo a respeitar os valores e os direitos da UE para garantir a credibilidade e continuidade do sistema (Csatlós, 2024; Fortes et al., 2022).

Outro dos dilemas mais recorrentes que relacionam o uso de tecnologia com a vigilância e privacidade é a 'espiral de securitização', conceito utilizado para justificar narrativas de segurança que impulsionam o desenvolvimento e uso de tecnologias, contribuindo para a militarização de práticas policiais (Balzacq, Léonard & Ruzicka, 2016; Bello, 2017), como são exemplo a utilização de tecnologias, como drones e vigilância biométrica que reflete, segundo Martins e Jumbert (2022), uma securitização das fronteiras da UE, transformando a migração num 'problema de segurança' tratável por soluções tecnológicas, criando dessa forma um paradoxo entre a necessidade de cuidado humanitário (neste caso aos refugiados) e o controlo rigoroso efetuado pelos países.

No mesmo sentido Gandhi (2024), indica que a utilização deste tipo de tecnologias pode melhorar a capacidade de detetar ameaças à segurança, mas ao mesmo tempo, pode levar à vigilância em massa e à violação de direitos fundamentais.

Babuta et al. (2018) também alertam para alguns cuidados na implementação destas tecnologias, sendo crucial garantir que os algoritmos sejam transparentes e inteligíveis, para que as suas decisões possam ser devidamente escrutinadas e compreendidas pois existe possibilidade de viés nos dados e, consequentemente, nos resultados dos algoritmos, que poderá levar a que o erro seja replicado e amplificado.

Por forma a mitigar alguns dos problemas identificados Fortes *et al.* (2022) indicam a necessidade de realizar 'testes de prudência'[76], para avaliar de forma exaustiva a adequação dos sistemas de decisão automatizada em contextos legais, sendo também indicadas por Gandhi (2024), uma revisão nas práticas de processamento de dados para melhorar a transparência nas organizações e uma maior supervisão por parte de órgãos como o *European Data Protection Supervisor*.

Por fim, importa destacar que a própria Comissão Europeia (2020) reconhece já há alguns anos a tensão entre a necessidade de segurança e a proteção da

[76] Inspirados nos testes de Alan Turing sobre "*Computing Machinery and Intelligence*".

privacidade dos cidadãos, indicando a necessidade a criação de um Fundamental *Rights Officer*[77], para garantir que as operações de segurança respeitem os direitos fundamentais, especialmente no uso de tecnologias emergentes como a IA.

4.3. Dilemas éticos e legais

Para além do desafio relacionado com a privacidade e vigilância, a 4RI terá um impacto significativo na sociedade e consequentemente no poder legislativo que terá também que se adaptar a uma série de outros desafios éticos e legais, muitos dos quais ainda estão a ser compreendidos[78]. Neste particular, Domingues (2020), introduz a problemática com alusão a uma série de questões que deverão merecer a nossa reflexão, tais como: até onde deve ir a legislação e a regulamentação para não obstruir a inovação e respeitar a liberdade individual e económica? Será possível legislar a neutralidade dos algoritmos na tomada de decisão e definir o enquadramento da sua responsabilidade civil[79]? Como conter a disseminação de ciberataques e notícias falsas que influenciam opiniões públicas e eleições, sem limitar a liberdade de expressão nas plataformas digitais?

Todas estas questões devem merecer a reflexão da sociedade, de modo a que os decisores políticos estabeleçam princípios e parâmetros regulatórios que garantam que a transformação em curso beneficie a sociedade como um todo.

Para dar resposta a algumas destas questões e por reconhecer que a IA tem um impacto significativo em vários setores da economia e da sociedade, incluindo a segurança, podendo trazer benefícios, mas também riscos, a UE está a adaptar-se e inclusive já criou uma regulamentação para garantir que a tecnologia seja usada de forma ética e segura – o Regulamento (UE) 2024/1689[80], que cria regras harmonizadas em matéria de IA.

Este marco legislativo fornece uma base sólida para analisar as implicações da IA, com especial atenção para os desafios éticos e legais e à proteção dos direitos fundamentais, e irá tornar-se um instrumento essencial para o enquadramento destas questões na Europa.

---

[77] Ação que já foi implementada por exemplo pela Frontex desde 2020.
[78] Por exemplo com a utilização dos dados online para fins políticos ou publicitários, como o escândalo que envolveu a *Cambridge Analytics,* mudou o mundo, mas não mudou o *Facebook* (Hern, 2019).
[79] Por exemplo, na condução autónoma, quem deverá ser responsabilizado num acidente com o veículo autónomo que mate alguém e quais os limites dessa responsabilidade em caso de acidente?
[80] O mesmo irá entrar em vigor em fevereiro de 2025, e tem de estar implementado até agosto de 2026 (https://digital-strategy.ec.europa.eu/pt/policies/regulatory-framework-ai).

Especificando agora a temática da análise preditiva, um dos dilemas associados à utilização de algoritmos é o conceito de 'deslocamento da discricionariedade' que segundo Brayne e Christin (2020) se refere à transferência do poder da decisão humanos para algoritmos, sendo crucial para entender como a adoção de tecnologias preditivas pode levar a uma redução aparente da discricionariedade humana, mas na prática, desloca-a para áreas menos sujeitas a escrutínio, como a manipulação de dados por parte de analistas ou a resistência passiva dos profissionais.

Sobre este particular é relevante mencionar igualmente a teoria da burocracia algorítmica (Bovens & Zouridis, 2002) pois descreve a transição de um policiamento baseado em interações humanas para um policiamento baseado em sistemas automatizados e algoritmos, levantando questões sobre a discricionariedade policial e a objetividade nas decisões, especialmente quando os algoritmos podem perpetuar vieses históricos presentes nos dados.

Como recomendações para a implementação destas tecnologias Brayne e Christin (2020), indicam que: (1) devem ser criados mecanismos de supervisão e auditoria para os algoritmos utilizados, que podem ajudar a garantir que as decisões baseadas em dados sejam justas e equitativas, (2) deve ser assegurada formação aos profissionais no uso dessas tecnologias para mitigar a resistência à implementação e (3) garantir que o conhecimento experiencial seja valorizado em conjunto com as análises algorítmicas.

Fortes *et al*. (2022), complementam que a regulação algorítmica deve também ser vista de forma ampla, especificando que a mesma deve abranger tanto a regulação de algoritmos como a regulação através de algoritmos, particularizando que a normatividade dos algoritmos não advém apenas do direito positivo, mas também da estrutura de comandos e consequências preditas nas suas fórmulas matemáticas, pelo que esta complexidade da regulação algorítmica deverá envolver múltiplos atores, como reguladores, regulados e terceiros, e diferentes formas de regulação (auto-regulação, co-regulação e meta-regulação).

Para além destes contributos, Lee et al. (2024) indicam que deve também ser ponderada, a potencial ameaça à democracia em termos de concentração de dados e poder nas mãos das autoridades policiais e tidas em conta eventuais tensões internas na própria organização policial decorrente da utilização destas novas tecnologias.

5. CONSIDERAÇÕES FINAIS

Conforme explanamos a 4RI está a desencadear uma transformação profunda na história da humanidade, com um impacto na segurança interna particularmente significativo.

Estes novos tempos são marcados de muitas promessas, necessidades de adaptação ao novo ecossistema tecnológico, mas também de potenciais ameaças e limitações éticas e legais.

Entre as principais oportunidades de transformação, na segurança interna, destacamos a possibilidade de modernização das práticas policiais através da automação de diversos processos, avaliações de risco e análise preditiva de dados em tempo real, nomeadamente com IA para melhorar a eficácia e eficiência das operações e análise preditiva de crimes, contudo, embora existam alegações e várias expectativas de que o policiamento preditivo pode reduzir a criminalidade e melhorar a eficiência policial, o que nos demostrou a revisão sistemática de Lee et al. (2024), efetuada a 161 estudos, é que a eficácia ainda não está comprovada devido ao reduzido número de estudos com aplicações em situações reais.

Foram também identificados diversos desafios, por um lado, relativamente à enorme quantidade de dados digitais, que para além das inúmeras possibilidades de uso, têm a limitação objetiva quando à capacidade de tratamento e análise, bem como, as ciberameaças que deverão ser tidas em conta na implementação de medidas de mitigação. Por outro, foram identificados um conjunto de dilemas éticos e legais na utilização de algoritmos, seja pelo risco de vieses, falta de transparência no funcionamento ou até mesmo discriminação, sendo crucial garantir que os mesmos sejam transparentes e inteligíveis, para que as decisões possam ser devidamente escrutinadas e compreendidas.

Em suma, os resultados desta investigação indicam que a 4RI pode oferecer oportunidades significativas para uma real modernização das forças de segurança e para uma otimização de recursos, contudo alerta-se também para a necessidade de regulamentação adequada e de uma abordagem estratégica na implementação destas tecnologias disruptivas pois a tecnologia por si só não garante o sucesso da inovação, sendo necessário um alinhamento com as mudanças organizacionais pretendidas.

As principais limitações desta investigação residiram abrangência do tema e na falta de dados empíricos sobre a implementação efetiva de algumas destas tecnologias no contexto policial. Para além disso, importa relevar dinâmica

acelerada das inovações, que pode tornar obsoletas, num curto espaço de tempo, algumas das tendências analisadas, pelo que se recomenda a realização de estudos sobre a implementação prática de tecnologias da 4RI na segurança interna, com foco na eficácia operacional, adesão institucional e na avaliação do impacto ético e legal.

REFERÊNCIAS BIBLIOGRÁFICAS

Afzal, M., & Panagiotopoulos, P. (2024). Data in policing: An integrative review. *International Journal of Public Administration, 47*(9), 1311-1330. https://doi.org/10.1080/01900692.2024.2360586

Babuta, A., & Oswald, M. (2018). Machine learning algorithms and police decision making. *Royal United Services Institute*. Disponível em https://www.rusi.org/explore-our-research/publications/whitehall-reports/machine-learning-algorithms-and-police-decision-making-legal-ethical-and-regulatory-challenges

Balzacq, T., Léonard, S., & Ruzicka, J. (2016). 'Securitization' revisited: Theory and cases. *International Relations, 30*(4), 494–531. https://doi.org/10.1177/0047117815596590

Beier, G., Ullrich, A., Niehoff, S., Reißig, M., & Habich, M. (2020). Industry 4.0: How it is defined from a sociotechnical perspective and how much sustainability it includes — A literature review. *Journal of Cleaner Production*, 259, 120856. https://doi.org/10.1016/j.jclepro.2020.120856

Bello, V. (2017). *International Migration and International Security. Why Prejudice is a Global Security Threat*. London: Routledge. https://doi.org/10.4324/9781315537634

Bovens, M., & Zouridis, S. (2002). From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and constitutional control. *Public Administration Review, 62*(2), 174–184. https://doi.org/10.1111/0033-3352.00168

Braga, A. A., & Bond, B. J. (2008). Policing crime and disorder hot spots: A randomized controlled trial. *Criminology, 46*(3), 577–607. https://doi.org/10.1111/j.1745-9125.2008.00124.x

Braga, A., Papachristos, A., & Hureau, D. (2012). Hot spots policing effects on crime. *Campbell Systematic Reviews, 8*(1), 1–90. https://doi.org/10.4073/csr.2012.8

Brayne, S. (2017). Big data surveillance: The case of policing. *American Sociological Review, 82*(5), 977–1008. https://doi.org/10.1177/0003122417725865

Brayne, S., & Christin, A. (2020). Technologies of crime prediction: The reception of algorithms in policing and criminal courts. *Social Problems, 67*(1), 1-17. https://doi.org/10.1093/socpro/spaa004

Carter, J. G., Mohler, G., Raje, R., Chowdhury, N., & Pandey, S. (2021). The Indianapolis harmspot policing experiment. *Journal of Criminal Justice, 74*, 101814. https://doi.org/10.1016/j.jcrimjus.2021.101814

Cetrulo, A., & Nuvolari, A. (2019). Industry 4.0: Revolution or hype? Reassessing recent technological trends and their impact on labour. *Journal of Industrial and Business Economics, 46*(3), 391–402. https://doi.org/10.1007/s40812-019-00132-y

Choo, K., Smith, G., & McCuster, R. (2007). The future of technology-enabled crime in Australia. *Trends & Issues in Crime & Criminal Justice, 341*. Canberra: Australian Institute of Criminology. Disponível em https://www.aic.gov.au/publications/tandi/tandi341

Comissão Europeia. (2020). Estratégia da UE para a União da Segurança. Disponível em https://ec.europa.eu/home-affairs/what-we-do/policies/internal-security_en

Conselho da UE. (2010). Estratégia de Segurança Interna da União Europeia: Rumo a um Modelo Europeu de Segurança. Luxemburgo: Serviço das Publicações da União Europeia. Disponível em: https://www.consilium.europa.eu/pt/documents-publications/publications/internal-security-strategy-european-union-towards-european-security-model/

Cremer, F., Wimmer, B., Pielmeier, M., Schallmo, D. A., & Kasperczyk, D. (2022). Cyber risk and cybersecurity: a systematic review of data. *Journal of Risk Research, 25*(5-6), 703-726. https://doi.org/10.1057/s41288-022-00266-6

Csatlós, E. (2024). Prospective implementation of AI for enhancing European (in) security. *European Journal of Migration and Law, 26*(1), 1-33. https://doi.org/10.1016/j.clsr.2024.105995

Domingues, S. (2020) Legislativo 4.0: O desafio da criação de novas leis para um mundo em mutação. Em Czymmeck, A (Ed.), *A quarta revolução industrial*. (pp. 35-58). Rio de Janeiro: Konrad Adenauer Stiftung.

Dressel, J., & Farid, H. (2018). The accuracy, fairness, and limits of predicting recidivism. Science Advances, 4(1). https://doi.org/10.1126/sciadv.aao5580

Ernst, R., Duysters, G., van Knippenberg, D., & Witte, H. D. (2021). Technological innovation in a police organization. Policing: *A Journal of Policy and Practice, 15*(1), 61-78. https://doi.org/10.1093/police/paab003

Europol. (2024). *Internet Organised Crime Threat Assessment (IOCTA) 2024*. Publications Office of the European Union. Disponível em https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024

Fortes, B., Baquero, M., & Restrepo D. (2022). Artificial intelligence risks and algorithmic regulation. *European Journal of Risk Regulation, 13*(3), 359-371. https://doi.org/10.1017/err.2022.14

Gandhi, S. (2024). Frontex as a hub for surveillance and data sharing: Challenges for data protection and privacy rights. *European Journal of Migration and Law, 26*(1), 35-61. https://doi.org/10.1016/j.clsr.2024.105963

Gouveia, J. (2020). *Direito da Segurança: Cidadania, Soberania e Cosmopolismo* (2.ª Ed.). Coimbra: Edições Almedina, S.A.

Hern, A. (2019). Cambridge Analytica: how did it turn clicks into votes? The Guardian. Disponível em https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie

Huang, C., Chou, T., & Wu, S. (2021). Towards convergence of AI and IoT for smart policing: A case of a mobile edge computing-based context-aware system. *Journal of Global Information Management, 29*(6), 1-21. https://doi.org/10.4018/JGIM.296260

Hunt, P., Saunders, J., & Hollywood, J. (2014). *Evaluation of the Shreveport predictive policing experiment*. Santa Monica: Rand Corporation. Disponível em https://www.rand.org/pubs/research_reports/RR531.html

Johnson, T., Johnson, N., McCurdy, D., & Olajide, M. (2022). Facial recognition systems in policing and racial disparities in arrests. *Government Information Quarterly, 39*(4), 101753. https://doi.org/10.1016/j.giq.2022.101753

Kaspersen, A. (2015, 08 de setembro). 8 emerging technologies transforming international security. World Economic Forum. Retirado de https://www.weforum.org/agenda/2015/09/8-technologies-transforming-international-security

Lee, K., Malerba, F., & Primi, A. (2020). The fourth industrial revolution, changing global value chains and industrial upgrading in emerging economies. *Journal of Economic Policy Reform, 23*(4), 359–370. https://doi.org/10.1080/17487870.2020.1735386

Lee, Y., Bradford, B., & Posch, K. (2024). The effectiveness of big data-driven predictive policing: Systematic review. *Justice Evaluation Journal, 7*(2), 127-160. https://doi.org/10.1080/24751979.2024.2371781

Loveday, B. (2017). Still plodding along? The police response to the changing profile of crime in England and Wales. *International Journal of Police Science & Management, 19*(2), 101–109. https://doi.org/10.1177/1461355717699634

Martins, B., & Jumbert, M. (2020). EU Border technologies and the co-production of security 'problems' and 'solutions'. *Journal of Ethnic and Migration Studies, 48*(6), 1430-1447. https://doi.org/10.1080/1369183X.2020.1851470

Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration, 42*(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664

Müller, J., Kiel, D., & Voigt, K. (2018). What drives the implementation of Industry 4.0? The role of opportunities and challenges in the context of sustainability. *Sustainability, 10*(1), 247. https://doi.org/10.3390/su10010247

OCDE. (2017). The next production revolution: Implications for governments and business. OECD Publishing. https://doi.org/10.1787/9789264271036-en

Oswald, M., Grace, J., Urwin, S., & Barnes, G. (2018). Algorithmic risk assessment policing models: Lessons from the Durham HART model and 'experimental' proportionality. *Information & Communications Technology Law, 27*(2), 223–250. https://doi.org/10.1080/13600834.2018.1458455

Perry, W. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. Rand Corporation. https://www.jstor.org/stable/10.7249/j.ctt4cgdcz

Ratcliffe, J., Taylor, R., Askey, A., Thomas, K., Grasso, J., Bethel, K., … Koehnlein, J. (2021). The Philadelphia predictive policing experiment. *Journal of Experimental Criminology, 17*(1), 15–41. https://doi.org/10.1007/s11292-019-09400-2

Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança). Jornal Oficial da União Europeia, L 151, 15-69.

Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial

e que altera os Regulamentos (CE) n.° 300/2008, (UE) n.° 167/2013, (UE) n.° 168/2013, (UE) 2018/858, (UE) 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). Jornal Oficial da União Europeia, L 1689, 12-69.

Sarmento, C. (2009). *Política e Segurança - Novas configurações do Poder*. Edições Almedina.

Saunders, J., Hunt, P., & Hollywood, J. (2016). Predictions put into practice: A quasi-experimental evaluation of Chicago's predictive policing pilot. *Journal of Experimental Criminology, 12*(3), 347–371. https://doi.org/10.1007/s11292-016-9272-0

Schwab, K. (2016). *The Fourth Industrial Revolution*. World Economic Forum.

Vomfell, L., Hardle, W., & Lessmann, S. (2018). Improving crime count forecasts using Twitter and taxi data. *Decision Support Systems, 113*, 73–85. https://doi.org/10.1016/j.dss.2018.07.003

Wyatt, T., & Alexander, M. (2010). The impact of predictive policing on traffic accidents in Nashville. *Journal of Traffic Safety, 12*(3), 45-60. https://doi.org/10.1016/j.trip.2021.100429

ESTUDO 5 – INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO: ANÁLISE E PREVENÇÃO DE CRIMES

ARTIFICIAL INTELLIGENCE IN PREDICTIVE POLICING: CRIME ANALYSIS AND PREVENTION

Pedro de Jesus Antunes Costa
Capitão GNR

RESUMO

No domínio da segurança pública, a Inteligência Artificial (IA) tem vindo a transformar os modelos tradicionais de atuação policial, permitindo o desenvolvimento de estratégias preditivas baseadas em dados. Este estudo analisa os desafios e oportunidades decorrentes da aplicação da IA no policiamento preditivo, com enfoque na sua contribuição para a análise e prevenção de crimes. Através de uma revisão bibliográfica sistemática, examinam-se as aplicações práticas da IA na segurança pública, os modelos preditivos e os impactos éticos, legais e operacionais. São abordadas tecnologias como reconhecimento facial, análise de hotspots, deteção automatizada de ameaças e sistemas de decisão baseados em machine learning. O estudo discute ainda a regulamentação europeia sobre IA, os riscos de enviesamento algorítmico e a importância da supervisão humana. Conclui-se que, embora a IA represente uma mais-valia na eficiência policial e na gestão estratégica de recursos, a sua implementação exige um quadro legal robusto, transparência e salvaguarda dos direitos fundamentais. Propõe-se o desenvolvimento de estudos empíricos no contexto nacional e mecanismos de controlo que assegurem a confiança pública e a legitimidade das forças de segurança na utilização destas tecnologias.

Palavras-chave: Inteligência Artificial; Policiamento Preditivo; Regulamentação; Direitos Fundamentais

ABSTRACT

In the field of public security, Artificial Intelligence (AI) has been transforming traditional policing models by enabling the development of data-driven predictive strategies. This study analyzes the challenges and opportunities arising from the application of AI in predictive policing, focusing on its contribution to crime analysis and prevention. Through a systematic literature review, the practical applications of AI in public security, predictive models, and their ethical, legal, and operational impacts are examined. Technologies such as facial recognition,

hotspot analysis, automated threat detection, and machine learning-based decision systems are addressed. The study also discusses European AI regulation, the risks of algorithmic bias, and the importance of human oversight. It concludes that although AI offers significant added value in police efficiency and strategic resource management, its implementation requires a robust legal framework, transparency, and the safeguarding of fundamental rights. The development of empirical studies in the national context and control mechanisms is proposed to ensure public trust and the legitimacy of security forces in the use of these technologies.

***Keywords**: Artificial Intelligence; Predictive Policing; Regulation; Fundamental Rights.*

1. INTRODUÇÃO

A segurança interna na União Europeia (UE) tem sido cada vez mais influenciada por desafios complexos, como o terrorismo e os fluxos migratórios, levando à adoção de novas estratégias de segurança pública (Hermenegildo, 2018). Nesse contexto, o desenvolvimento da IA tem vindo a revolucionar os paradigmas operacionais das forças de segurança. A IA evidencia, atualmente, um potencial extraordinário no âmbito da segurança pública, constituindo-se como um instrumento fundamental na prevenção criminal (Comissão Europeia, 2019, 2020; Telles, 2021; Ramos, 2023).

A capacidade da IA para processar e analisar grandes volumes de dados possibilitou o desenvolvimento do policiamento preditivo, uma abordagem baseada na análise estatística de padrões criminais que permite estimar a probabilidade de ocorrências criminais futuras, baseando-se em dados históricos e fatores ambientais (Moleirinho et al., 2024). A integração da IA no policiamento representa uma transição significativa dos modelos tradicionais para uma abordagem orientada por dados, possibilitando uma alocação mais eficiente de recursos e estratégias preventivas mais robustas (Pearson, Adey, & Jensen, 2024; Europol, 2024).

Não obstante os evidentes benefícios operacionais, a implementação da IA no contexto do policiamento preditivo suscita desafios substanciais. Questões prementes como a fiabilidade dos dados, os enviesamentos algorítmicos e as implicações ético-jurídicas têm sido objeto de amplo debate académico (Floridi & Cowls, 2019; Brayne, 2021). O Regulamento da IA, publicado a 12 de julho de 2024, estabelece-se como o primeiro quadro jurídico da UE neste domínio, instituindo diretrizes fundamentais para assegurar uma aplicação ética da IA em consonância com os direitos fundamentais (Parlamento Europeu e Conselho da União Europeia,

2024; Europol, 2024). A entrada em vigor das disposições relativas às práticas proibidas de IA, a 2 de fevereiro de 2025, demonstra a importância de uma análise aprofundada deste instrumento normativo (Parlamento Europeu e Conselho da União Europeia, 2024).

Face a este enquadramento, emerge a seguinte questão central de investigação: Quais são os desafios e oportunidades decorrentes da aplicação da Inteligência Artificial no policiamento preditivo? Para responder a esta questão, o presente estudo propõe-se analisar os benefícios operacionais da IA, bem como os desafios éticos, legais, técnicos e operacionais inerentes à sua implementação no domínio do policiamento preditivo.

A metodologia adotada assenta numa revisão bibliográfica sistemática, recorrendo à análise de conteúdo preconizada por Bardin (1997). O corpus documental contempla estudos académicos, relatórios institucionais e instrumentos normativos, com particular incidência na legislação europeia e documentos emanados de organizações de referência como a Europol, o *Government Accountability Office* (GAO) dos Estados Unidos da América (EUA) e a Organização para a Segurança e Cooperação na Europa (OSCE), proporcionando uma perspetiva abrangente e internacional sobre o impacto da IA no policiamento preditivo.

O presente trabalho encontra-se estruturado em cinco secções distintas. A introdução contextualiza a problemática em análise. A segunda secção examina a evolução histórica da IA e do policiamento preditivo. A terceira secção debruça-se sobre as aplicações práticas da IA no domínio do policiamento preditivo. A quarta secção analisa o enquadramento regulamentar e os impactos éticos, legais, técnicos e operacionais, ponderando os desafios e oportunidades emergentes. Por fim, a conclusão sintetiza as principais inferências e apresenta recomendações para investigações futuras.

2. A INTELIGÊNCIA ARTIFICIAL E O POLICIAMENTO PREDITIVO

2.1. Definição e evolução da inteligência artificial

A IA tem as suas origens na década de 1940, quando Warren McCulloch e Walter Pitts criaram o primeiro modelo computacional para redes neurais, aplicando lógica matemática para representar processos cognitivos. No entanto, o termo "inteligência artificial" foi formalmente introduzido apenas em 1956, durante a Conferência de Dartmouth, por John McCarthy (Russell & Norvig, 2010).

Embora não haja uma definição única e consensual para IA, diversas abordagens refletem a sua complexidade e aplicação multidisciplinar. A UE, no artigo 3.º do Regulamento da IA, descreve-a como um "sistema baseado em máquinas concebido para operar com diferentes níveis de autonomia [...] capaz de inferir resultados como previsões, recomendações ou decisões que possam afetar ambientes físicos ou virtuais" (Parlamento Europeu e Conselho da União Europeia, 2024, p. 46). Da mesma forma, Floridi e Cowls (2019, p. 3, nossa tradução) definem a IA como "a capacidade de máquinas realizarem tarefas que normalmente exigiriam inteligência humana, incluindo aprendizagem, raciocínio e tomada de decisões".

Desde a sua conceção, a IA evoluiu significativamente, passando de sistemas baseados em regras fixas para modelos dinâmicos que incorporam *machine learning* e *big data*, permitindo análises mais precisas e predições avançadas (Andrade, 2022; Ramos, 2023; Magalhães et al., 2024). A crescente capacidade computacional e a exploração intensiva de dados têm ampliado a aplicabilidade da IA em diferentes domínios, incluindo a segurança pública (Floridi & Cowls, 2019; Comissão Europeia, 2019, 2020).

No âmbito do policiamento, a IA tem sido utilizada para otimizar operações, reforçando a eficiência das forças de segurança na análise criminal e na prevenção de crimes (Ratcliffe, 2003; Meijer & Wessels, 2019; Europol, 2024). A adoção de *big data* e algoritmos preditivos permitiu identificar padrões de criminalidade e antecipar cenários de risco, facilitando a alocação de recursos estratégicos (Europol, 2024; Ferguson, 2020; Moleirinho et al., 2024).

Apesar dos avanços, a IA enfrenta desafios técnicos e operacionais, incluindo a qualidade dos dados, a transparência dos algoritmos e o risco de enviesamento algorítmico (GAO, 2018; Moleirinho et al., 2024). Para mitigar riscos e garantir um uso ético da tecnologia, a UE tem promovido regulamentações rigorosas, que também serão alvo de estudo. Dessa forma, a IA apresenta um enorme potencial para melhorar a segurança pública, mas a sua implementação exige supervisão eficaz e regulamentação clara para mitigar riscos e garantir uma utilização alinhada com princípios éticos e jurídicos.

2.2. A EVOLUÇÃO DO POLICIAMENTO E A NECESSIDADE DE NOVAS FERRAMENTAS

A necessidade de modernização das forças de segurança levou ao desenvolvimento de ferramentas tecnológicas mais avançadas. A IA e a análise

preditiva emergem como soluções estratégicas para otimizar os processos de policiamento e a alocação de recursos (Telles, 2021). Tecnologias como os Sistemas de Informação Geográfica (SIG) contribuem para a identificação de padrões criminais, direcionando operações com maior precisão e eficiência (Ratcliffe, 2004).

A IA tem sido amplamente aplicada na previsão de locais de alto risco para crimes, auxiliando na tomada de decisões estratégicas. Além disso, a IA pode ser utilizada para detetar propaganda terrorista, identificar transações suspeitas e auxiliar equipas de emergência na gestão de crises (Comissão Europeia, 2020).

Contudo, a implementação da IA no policiamento preditivo requer transparência e supervisão rigorosa (Ferguson, 2020). O GAO (2018) alerta que a qualidade dos dados e a proteção da privacidade são determinantes para garantir a confiabilidade dos sistemas baseados em IA. Dados imprecisos ou enviesados podem comprometer a eficácia dos algoritmos, gerando impactos negativos na aplicação da lei (Meijer & Wessels, 2019; Brayne, 2021).

Outro desafio significativo está relacionado com as implicações éticas e com o impacto na privacidade dos cidadãos. Moleirinho et al. (2024) destacam que o aumento da vigilância baseada em IA pode comprometer direitos fundamentais, exigindo regulamentações rigorosas para evitar abusos e garantir um equilíbrio entre segurança e liberdade individual.

Apesar dos desafios, a adoção da IA no policiamento representa um avanço significativo na segurança pública. Aplicadas de forma ética e supervisionada, essas tecnologias promovem maior eficiência operacional e reforçam a cooperação entre forças de segurança e comunidades. Estudos indicam que iniciativas que combinam inovação tecnológica e participação comunitária melhoram a perceção pública e aumentam a legitimidade institucional das forças policiais (Europol, 2024; Wuschke et al., 2018).

Assim, a evolução do policiamento exige uma abordagem equilibrada, na qual a tecnologia seja empregue estrategicamente. A IA e a análise preditiva apresentam um elevado potencial para reforçar a segurança interna, desde que implementadas sob um quadro legal sólido e supervisionado.

2.3. A INTELIGÊNCIA ARTIFICIAL PARA AS ESCOLAS DE PENSAMENTO DA SEGURANÇA

As escolas de pensamento no domínio da segurança fornecem alicerces teóricos essenciais para compreender o impacto da IA na segurança pública e

no policiamento preditivo. A europeização da segurança interna e a crescente interdependência entre os Estados-Membros têm impulsionado a adoção de tecnologias emergentes para fortalecer a gestão de riscos e ameaças (Hermenegildo, 2013). Neste contexto, o policiamento contemporâneo, alicerçado na inteligência, privilegia a análise sistemática de dados como base para a formulação de decisões estratégicas (OSCE, 2017).

O policiamento preditivo está diretamente relacionado com abordagens como o policiamento orientado pela inteligência e o policiamento baseado na resolução de problemas, inserindo-se num paradigma que abrange o policiamento comunitário e a abordagem situacional. Estas metodologias destacam a importância da análise dos fatores sociais e ambientais na prevenção criminal (Ratcliffe, 2003; Brantingham *et al.*, 2005).

No âmbito desta análise, a Escola de Copenhaga, ao introduzir o conceito de securitização, enfatiza que determinadas questões podem ser convertidas em ameaças para justificar medidas excecionais (Wæver, 1998). Segundo Wæver (1998), a segurança não é uma condição objetiva, mas sim um instrumento político, utilizado para legitimar ações estatais. Complementando esta visão, Buzan (1998) identifica desafios como a proliferação das novas tecnologias e as mudanças nas relações de poder, que redefinem a segurança no século XXI. Como sublinha Huysmans (2006, citado em Hermenegildo, 2018, p. 150), "a insegurança não é um facto natural, mas exige sempre que seja escrita e falada a sua existência".

Por seu turno, a Escola de Paris foca-se na instrumentalização das tecnologias de vigilância, nomeadamente no controlo da imigração e do terrorismo. Bigo (2002) argumenta que a securitização da imigração resulta do desenvolvimento das tecnologias de controlo e não o contrário. Esse fenómeno pode conduzir à normalização da vigilância massiva e a abordagens discriminatórias. Como sustenta Bigo (1998, citado em Hermenegildo, 2013, p. 163), "o contínuo de segurança inclui o controlo das fronteiras e da imigração dentro das atividades policiais da luta contra o crime". Nesta linha, Bigo, Isin, & Ruppert (2019) reforçam que os dados não são neutros, mas sim construídos por fatores sociais, políticos e económicos, salientando que a crescente cooperação transnacional na área da segurança desafia os conceitos tradicionais de soberania nacional e a relação Estado-cidadão.

Na análise das diferentes correntes teóricas, Foucault (2008) evidencia os conceitos de governamentalidade e biopoder, descrevendo como os Estados mobilizam tecnologias para monitorização populacional. A convergência entre

segurança interna e externa, impulsionada pela inovação tecnológica, amplia a capacidade de controlo do Estado. Neste contexto, a IA surge como uma ferramenta que fortalece a vigilância algorítmica, permitindo a antecipação e resposta automatizada a potenciais ameaças (Foucault, 2008).

Neste contexto, ao enfatizar os impactos sociais e éticos da IA no policiamento, o Regulamento da IA estabelece critérios rigorosos para assegurar a transparência e equidade na implementação destes sistemas (Parlamento Europeu e Conselho da União Europeia, 2024). Paralelamente, a Europol (2024) e Moleirinho (2021) destacam o potencial transformador da IA na segurança pública, mas alertam para desafios éticos e jurídicos, sobretudo no que diz respeito à privacidade e à proteção de dados. Esta realidade reforça a perspetiva de Walt (1991), que reconhece que as tecnologias emergentes desafiam os conceitos tradicionais de segurança, exigindo novos paradigmas preventivos.

Da análise comparativa das diversas escolas de pensamento em matéria de segurança, infere-se que a utilização de novas tecnologias redefine substancialmente a relação entre Estado e indivíduos. Não obstante as distinções conceptuais assentes no discurso securitário, no controlo e vigilância, e nos conceitos de governamentalidade e biopoder, constata-se que a aplicação da IA no policiamento preditivo requer uma análise multifacetada, que concilie inovação tecnológica com regulamentação e supervisão adequadas. A operacionalização destas ferramentas exige uma abordagem crítica e multidisciplinar que salvaguarde o respeito pelos direitos fundamentais.

3. APLICAÇÕES DA INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO

3.1. O POLICIAMENTO PREDITIVO: EVOLUÇÃO E O PAPEL DA INTELIGÊNCIA ARTIFICIAL

O policiamento preditivo representa uma transformação significativa na forma como as forças de segurança abordam a prevenção e a investigação criminal. Tradicionalmente baseado em respostas reativas, este modelo representa uma mudança para uma abordagem proativa que recorre à análise preditiva para identificar padrões criminais e otimizar a alocação de recursos (Mandalapu et al., 2023; Pearson, Adey, & Jensen, 2024; Wuschke et al., 2018). Telles (2021) sublinha que os modelos matemáticos e estatísticos otimizam a análise preditiva, permitindo uma gestão mais eficiente das forças policiais.

O mapeamento do crime evoluiu de simples marcações em mapas de papel para complexos SIG. Estes sistemas são ferramentas que utilizam hardware, software, pessoas e organizações para recolher, analisar e disseminar informação geográfica (Ratcliffe, 2004). A evolução do policiamento preditivo reflete-se na adoção de modelos estatísticos e algoritmos que identificam *hotspots* criminais e antecipam comportamentos suspeitos, orientando a tomada de decisões policiais (Meijer & Wessels, 2019; Ratcliffe, 2004). O mapeamento de *hotspots* tem sido um exemplo fundamental, direcionando operações para áreas de maior risco e reduzindo a incidência de crimes (Proença, 2023; Ratcliffe, 2004).

A forte capacidade de análise de dados é um dos pilares do policiamento orientado pela inteligência, sendo o avanço do *big data*, *machine learning* e da IA determinante para esse desenvolvimento, permitindo a análise de grandes volumes de dados para prever a ocorrência de crimes (Ratcliffe, 2004; Bostrom, 2014; Ferguson, 2017). O uso de big data permite detetar padrões ocultos nos registos criminais históricos, contribuindo para estratégias preventivas mais eficazes (Ferguson, 2017; Moleirinho 2021).

A IA aplicada ao policiamento preditivo tem impacto na eficiência operacional ao analisar dados criminais históricos, informações socioeconómicas e outras variáveis para prever onde os crimes são mais prováveis de ocorrer (GAO, 2018; Europol, 2024). Algumas destas tecnologias têm demonstrado impacto na redução da criminalidade patrimonial, evidenciando o potencial da IA para fortalecer a prevenção e a gestão eficiente dos recursos policiais (Meijer & Wessels, 2019).

Além da previsão de crimes e da otimização dos patrulhamentos, a IA tem sido utilizada para avaliar riscos e identificar indivíduos de interesse. Brayne (2021) refere que departamentos de polícia utilizam pontuações de risco baseadas em fatores como histórico criminal e afiliações a gangues para orientar investigações e operações preventivas. No entanto, essa prática levanta preocupações éticas, particularmente no que diz respeito à transparência e ao risco de discriminação algorítmica. A Europol (2024) alerta que, se os dados forem enviesados, os algoritmos podem perpetuar desigualdades sociais e comprometer a confiança pública na aplicação da lei.

A integração da IA no policiamento preditivo exige supervisão rigorosa e mecanismos de salvaguarda ética. Andrade (2022) destaca que a eficácia dessas ferramentas depende da qualidade e integridade dos dados, bem como da existência de auditorias que garantam responsabilização e clareza. A regulamentação é um

fator essencial para mitigar riscos, assegurando que a tecnologia seja aplicada de forma equilibrada e respeitadora dos direitos fundamentais (Parlamento Europeu e Conselho da União Europeia, 2024).

Apesar dos benefícios operacionais, o policiamento preditivo ainda carece de regulamentação específica em vários países, incluindo Portugal. Rodrigues, Fidalgo & Pais (2022) indicam que, em Portugal, não há uma definição formal de policiamento preditivo, mas o conceito envolve o uso de IA para prever comportamentos criminais e identificar potenciais agentes e locais de ocorrência. O Ministério da Ciência, Tecnologia e Ensino Superior (2019) reconhece a IA como uma ferramenta para otimizar a eficiência dos serviços públicos, incluindo as forças de segurança. Contudo, a adoção dessas tecnologias exige debate público e supervisão legal para equilibrar inovação e proteção dos direitos individuais. Assim, o policiamento preditivo, quando implementado de forma ética e regulamentada, pode ser uma ferramenta valiosa para a segurança pública, contribuindo para a redução da criminalidade e a melhoria da eficiência das forças policiais.

3.2. Aplicações da inteligência artificial na análise e prevenção de crimes

A aplicação da IA na análise e prevenção de crimes tem transformado a atuação das forças de segurança, permitindo abordagens preditivas mais eficientes. Entre as principais aplicações, destacam-se o reconhecimento facial, a análise de padrões criminais e a previsão de áreas de risco, que otimizam a resposta das autoridades e contribuem para uma segurança pública mais proativa (Europol, 2024; Ferguson, 2017; Moleirinho, 2021; Olaoye & Egon, 2024).

Uma das aplicações mais debatidas da IA na segurança pública é o reconhecimento facial, amplamente utilizado para identificar indivíduos procurados pela justiça em eventos de grande escala. O uso de biometria e IA tem sido adotado para investigações criminais, reduzindo o tempo de resposta e aumentando a eficiência operacional (Europol, 2024).

O mapeamento de *hotspots* criminais, através de SIG, tem sido amplamente utilizado para otimizar operações policiais (Ratcliffe, 2004; Telles, 2021). Os modelos de *machine learning* processam grandes volumes de dados para detetar correlações que não seriam identificáveis por métodos tradicionais, sendo utilizados para prever riscos e otimizar estratégias de patrulhamento (Mandalapu et al., 2023; Telles, 2021). Um exemplo relevante é o *PredPol*, um software adotado

nos EUA que analisa padrões criminais históricos para prever novas ocorrências e direcionar patrulhamentos para áreas de maior risco (Brayne, 2021). Embora tenha demonstrado eficácia na redução da criminalidade, alguns estudos apontam que o *PredPol* pode reforçar padrões de policiamento seletivo se os dados forem enviesados (Meijer & Wessels, 2019). Outra ferramenta inovadora é o *ShotSpotter*, inicialmente desenvolvido para deteção de terramotos nos EUA, mas que foi adaptado para identificar disparos em tempo real, possibilitando uma resposta policial mais célere e eficaz (Telles, 2021).

No campo da prevenção, a IA tem sido utilizada na análise de redes sociais para identificar comportamentos suspeitos e potenciais ameaças e no controlo rodoviário, auxiliando na deteção de padrões de sinistralidade rodoviária e implementando medidas preventivas (Barroca, 2021; Moleirinho 2021; Ramos, 2023).

A Europol (2024) destaca ainda a utilização da IA na análise de texto e linguagem natural, que permite que os computadores compreendam a linguagem humana, e na área digital forense, na qual a IA auxilia na análise de dispositivos digitais, como *smartphones* e computadores, recuperando dados apagados, analisando padrões e identificando atividades criminosas ou ilegais.

No contexto europeu, a utilização de SIG também tem demonstrado resultados promissores (Brantingham et al., 2005; Moleirinho et al., 2024; Meijer & Wessels, 2019). Assim, na Europa, destaca-se o projeto *Artificial Intelligence and advanced Data Analytics* (AIDA), financiado pelo programa Horizonte 2020 da UE, que se foca na análise de dados para a investigação criminal (Ramos, 2023). Além deste, os projetos financiados pela UE, *Anfi-FinTer*, que se concentra no combate ao financiamento do terrorismo através do rastreamento de atividades na dark web e ativos criptográficos e o *iBorderCtrl* que usa a deteção de emoções para desenvolver um sistema de apoio à decisão para os controlos fronteiriços, são exemplos relevantes (Magalhães et al., 2024).

Em Portugal, algumas forças e serviços de segurança já implementaram iniciativas semelhantes. A Guarda Nacional Republicana (GNR), em parceria com a Universidade de Évora, desenvolveu um projeto de IA para prever e reduzir a sinistralidade rodoviária no distrito de Setúbal, utilizando análise preditiva para otimizar a fiscalização e intervenção preventiva (TSF, 2019). Paralelamente, a Polícia Judiciária participa em projetos europeus como STARLIGHT, GRACE e DARLENE, aplicando IA à investigação criminal e à segurança pública, reforçando a identificação de padrões criminosos e a prevenção de delitos graves (Polícia

Judiciária, 2021, 2022). Estas iniciativas demonstram a crescente integração da IA na modernização das estratégias policiais e na adaptação das forças de segurança aos desafios tecnológicos contemporâneos.

Apesar das vantagens proporcionadas pela IA, a sua implementação levanta preocupações éticas e legais, como o risco de enviesamento algorítmico e impacto na privacidade individual (Europol, 2024). Para mitigar estes riscos, o Regulamento da IA exige que as autoridades assegurem a exatidão, fiabilidade e transparência dos sistemas de IA, além de realizar avaliações de impacto sobre os direitos fundamentais antes da sua implementação (Parlamento Europeu e Conselho da União Europeia, 2024). Assim, as aplicações da IA na análise e prevenção de crimes demonstram um enorme potencial para transformar o policiamento, tornando-o mais eficaz, estratégico e proativo. No entanto, os desafios éticos e legais associados ao seu uso exigem regulamentação clara e supervisão rigorosa.

4. IMPACTOS DA INTELIGÊNCIA ARTIFICIAL NO POLICIAMENTO PREDITIVO

4.1. Necessidades de regulamentação e supervisão

A regulamentação da IA no policiamento preditivo é essencial para assegurar que estas tecnologias sejam aplicadas de forma ética, transparente e responsável. O Parlamento Europeu continua a alertar para os riscos do viés algorítmico, a necessidade de supervisão humana e bases legais robustas para mitigar discriminações no uso da IA em segurança pública (Andrade, 2022; Hoadley & Lucas, 2018; Zenor, 2021). A Europol (2024) enfatiza que o desenvolvimento da IA deve ser pautado por princípios de transparência, segurança e inclusão, garantindo que as decisões automatizadas possam ser auditadas e explicadas.

Além das implicações legais, o uso da IA levanta preocupações éticas relacionadas com viés de dados, justiça, privacidade e direitos humanos. O Ministério da Ciência, Tecnologia e Ensino Superior (2019), na sua estratégia para a IA 2030, destaca a necessidade de um debate público sobre os impactos da IA na segurança pública, assegurando que o seu desenvolvimento esteja alinhado com princípios democráticos. Como apontam Meijer & Wessels (2019), a dificuldade de responsabilização destas tecnologias reforça a necessidade de regulamentação mais abrangente. A governança da IA deve centrar-se na proteção dos cidadãos e na promoção da confiança pública (AMA, 2022).

Neste âmbito, a UE tem procurado estabelecer um regime jurídico harmonizado que assegure a aplicação da IA em conformidade com o interesse público. O Regulamento da IA classifica os sistemas em diferentes níveis de risco, proibindo aqueles que representam risco inaceitável, como os sistemas de categorização biométrica e de avaliação preditiva de crimes baseada exclusivamente em perfis individuais, de acordo com o seu artigo 5.º. No entanto, prevê exceções para autoridades responsáveis pela aplicação da lei, permitindo o uso de sistemas de risco elevado sob requisitos rigorosos de transparência, supervisão humana e avaliação do impacto nos direitos fundamentais e em conformidade com os direitos da UE e nacionais, conforme estabelecido no ponto 6, alínea d), do Anexo III). (Parlamento Europeu e Conselho da União Europeia, 2024).

Portugal está entre os países que aprovaram, em 2025, o uso destas tecnologias, defendendo que restrições excessivas não devem comprometer a atuação das forças policiais (Executive Digest, 2025; Público, 2025). Dado o impacto desta regulamentação, e face à inexistência de uma entidade reguladora específica para estas matérias, em Portugal, a Autoridade Nacional de Comunicações (ANACOM) coordenou recentemente a primeira reunião das entidades responsáveis pela supervisão da IA de risco elevado, promovendo cooperação e partilha de informações sobre regulamentação e segurança (IGSJ, 2025).

De acordo com a Comissão Europeia (2019), a tecnologia deve ser desenvolvida de forma ética e fiável, prevenindo danos não intencionais. Além disso, as lógicas de governação da segurança pública são dinâmicas e influenciadas por fatores políticos e sociais (Bossong & Hegemann, 2018).

Assim, regulamentações claras e mecanismos eficazes de supervisão são fundamentais para maximizar os benefícios da IA e mitigar os seus riscos. A Europol (2024) alerta para a necessidade de restringir o uso destas ferramentas a casos devidamente justificados, garantindo um equilíbrio entre segurança e privacidade. O Livro Branco sobre IA destaca ainda a necessidade de diretrizes para a proteção de dados pessoais e prevenção da discriminação (Comissão Europeia, 2020). A implementação bem-sucedida da IA no policiamento preditivo dependerá, assim, da adoção de práticas de responsabilização, assegurando que a tecnologia seja utilizada com base em valores democráticos e respeito pelos direitos fundamentais.

4.2. Questões éticas e legais

A implementação da IA no policiamento preditivo levanta desafios significativos no que concerne à proteção de dados, privacidade e equidade.

Embora estas tecnologias possam otimizar a prevenção e a investigação criminal, a sua utilização exige regulamentação rigorosa e supervisão adequada para garantir o respeito pelos direitos fundamentais (Europol, 2024; OSCE, 2017; Moleirinho et al., 2024; Wuschke et al., 2018).

A proteção de dados pessoais é um direito fundamental e um dos principais desafios da IA aplicada ao policiamento. De acordo com a Diretiva (UE) 2016/680, os dados pessoais devem ser recolhidos apenas para finalidades legítimas e em conformidade com elevados padrões de segurança (Parlamento Europeu e Conselho da União Europeia, 2016). Esta diretiva está alinhada com o disposto nos Artigo 12.º da Declaração Universal dos Direitos Humanos (Nações Unidas, 1948) e Artigo 8.º da Convenção Europeia dos Direitos Humanos (Conselho da Europa, 1950), que estabelecem garantias ao direito à privacidade e contra intromissões arbitrárias na vida privada. Além disso, a Carta Portuguesa de Direitos Humanos na Era Digital, no seu artigo 9.º, exige que a IA respeite os princípios de transparência, segurança e responsabilidade, prevenindo preconceitos e discriminação algorítmica (Assembleia da República, 2021).

A Europol (2024) alerta para os riscos da IA no policiamento, incluindo a privacidade dos dados e a integridade das decisões automatizadas. Tecnologias como reconhecimento facial, biometria e vigilância massiva geram preocupações sobre potenciais abusos e exigem regulamentação para evitar violações de direitos fundamentais (Barroca, 2021). Além disso, os algoritmos preditivos podem desafiar conceitos jurídicos como a presunção de inocência, ao basearem ações policiais em probabilidades estatísticas em vez de provas concretas (Andrade, 2022; Brayne, 2021). A ausência de transparência nos sistemas de IA e a falta de mecanismos de responsabilização podem ainda comprometer a confiança pública e acentuar desigualdades na aplicação da lei (Meijer & Wessels, 2019; Zenor, 2021).

O Regulamento da IA classifica determinados usos da IA no policiamento como de risco elevado, impondo requisitos rigorosos de supervisão, transparência e auditoria. No entanto, o Regulamento exclui do seu âmbito sistemas de IA usados para fins militares, de defesa e segurança nacional. Se um sistema inicialmente desenvolvido para esses fins for posteriormente aplicado em contextos civis ou policiais, passa a estar sujeito às regras do regulamento (Parlamento Europeu e Conselho da União Europeia, 2024).

A distinção entre segurança nacional e segurança interna nos Estados-Membros da UE gera desafios interpretativos na aplicação da IA. Em Portugal, a segurança nacional não possui uma definição legal específica, ao contrário da segurança interna, que se centra na ordem pública e na proteção dos cidadãos,

conforme definido na Lei de Segurança Interna (Assembleia da República, 2008). Vários autores definem segurança nacional como a proteção da soberania, da integridade territorial e dos valores nacionais (Cardoso, 1981; Fonseca, 2010; Hoadley & Lucas, 2018). A ausência de um enquadramento legal claro pode criar ambiguidades na aplicação de sistemas de IA para fins de vigilância, policiamento e análise preditiva, influenciando a forma como são implementados nos diferentes países.

Para garantir um equilíbrio entre segurança e direitos fundamentais, a aplicação da IA no policiamento preditivo exige um quadro legal robusto, auditorias independentes e supervisão democrática. Adicionalmente, é essencial fomentar mecanismos de participação pública, permitindo que os cidadãos acompanhem e fiscalizem o uso destas tecnologias (Barroca, 2021). A IA pode transformar a segurança pública, mas apenas se for aplicada de forma ética, transparente e respeitadora dos direitos fundamentais.

4.3. Aspetos técnicos e operacionais

A implementação da IA no policiamento preditivo envolve desafios técnicos e operacionais que influenciam diretamente a sua eficácia e aplicabilidade. A capacidade dos algoritmos para analisar padrões criminais, prever *hotspots* e otimizar a alocação de recursos depende da qualidade dos dados, da capacidade computacional e da integração eficiente com as práticas operacionais das forças de segurança (Ferreira et al., 2012; GAO, 2018). Segundo Ferreira et al. (2012, p. 36, nossa tradução), "o policiamento preditivo baseia-se na análise e na avaliação do risco, sendo a qualidade dos dados essencial para a eficácia dos modelos preditivos". No entanto, desafios como a atualização deficiente das bases de dados, o treino inadequado dos modelos e dificuldades na sua integração com sistemas operacionais existentes comprometem a fiabilidade das previsões (Ferreira *et al.*, 2012; GAO, 2018).

Os modelos preditivos podem contribuir significativamente para um policiamento mais eficiente, reduzindo custos operacionais e otimizando a alocação de recursos (Mandalapu et al., 2023). Algoritmos de *machine learning*, são amplamente utilizados para prever padrões criminais e permitir decisões estratégicas baseadas em dados (Mandalapu et al., 2023). Contudo, a eficácia desses modelos depende da sua calibração contínua, minimizando riscos associados ao viés algorítmico e garantindo que as previsões reflitam padrões criminais reais, e não desigualdades

estruturais ou práticas discriminatórias (Mandalapu et al., 2023; Ratcliffe, 2003).

A integração da IA nos sistemas policiais requer não apenas infraestruturas tecnológicas, mas também alterações organizacionais. A interoperabilidade entre bases de dados, a formação contínua dos agentes e a transparência nos processos de tomada de decisão são essenciais para evitar erros sistémicos e garantir o uso responsável da tecnologia. A governança e regulamentação legal também desempenham um papel determinante, pois a implementação de auditorias regulares e mecanismos de responsabilização contribui para a confiança na tecnologia e para a sua utilização ética (Barroca, 2021; AMA, 2022).

Além disso, a falta de conhecimento técnico entre os decisores estratégicos pode dificultar a maximização do potencial da IA no policiamento preditivo. A análise de dados deve ser compreendida e aplicada de forma adequada, permitindo que a tecnologia seja utilizada como ferramenta de apoio à tomada de decisões operacionais (Ratcliffe, 2004). O policiamento preditivo tem revolucionado a forma como os recursos policiais são alocados e pode maximizar a eficiência operacional e direcionar ações preventivas (Brayne, 2021). No entanto, a automação excessiva pode reduzir a autonomia dos agentes no terreno, comprometendo a sua capacidade de julgamento em situações específicas e sensíveis (Ratcliffe, 2004; Comissão Europeia, 2019; Pedroso & Santos, 2024).

Outro fator crítico é o potencial de autoaperfeiçoamento da IA, que pode trazer vantagens operacionais, mas também desafios técnicos, uma vez que a capacidade de auto-otimização pode aumentar a complexidade dos sistemas de policiamento preditivo, exigindo monitorização constante para evitar desvios ou falhas imprevistas (Bostrom, 2014). A evolução desses sistemas levanta a necessidade de um controlo rigoroso, assegurando que a IA permaneça alinhada aos princípios éticos e aos objetivos das forças de segurança (Bostrom, 2014).

Apesar dos desafios, a IA apresenta oportunidades substanciais para tornar o policiamento mais orientado por dados, melhorando a gestão dos recursos disponíveis e aumentando a capacidade de antecipação de riscos.

4.4. Desafios e oportunidades da inteligência artificial no policiamento preditivo

A implementação da IA no policiamento preditivo representa um avanço significativo na segurança pública, permitindo otimizar recursos e prever padrões criminais. No entanto, as questões éticas, legais e técnicas exigem um

enquadramento robusto para garantir transparência e equidade no seu uso (Parlamento Europeu e Conselho da União Europeia, 2024).

Um dos desafios centrais é a qualidade e fiabilidade dos dados. Os modelos preditivos dependem da precisão das bases de dados, e informações enviesadas podem reforçar discriminações estruturais e reforçar estereótipos preexistentes (Pedroso & Santos, 2024; Andrade, 2022). Além disso, a falta de validação empírica levanta dúvidas sobre a real eficácia desses sistemas na redução da criminalidade (Meijer & Wessels, 2019). Em complemento, alguns indicadores tradicionais de eficácia policial, como taxas de resolução de crimes, podem ser manipuláveis e não refletir adequadamente a contribuição das tecnologias para a segurança pública (Baughman, 2020).

A regulamentação da IA é outro desafio fulcral. O Regulamento da IA impõe diretrizes para garantir auditoria, supervisão humana e proteção da privacidade, procurando equilibrar inovação tecnológica com a proteção dos direitos fundamentais (Parlamento Europeu e Conselho da União Europeia, 2024). Contudo, a centralização de dados sensíveis e a opacidade dos algoritmos continuam a gerar preocupações sobre a responsabilização e possíveis abusos (Europol, 2024; Zenor, 2021). A IA deve operar dentro de um quadro legal que proteja a privacidade dos cidadãos e evite vigilância excessiva (Comissão Europeia, 2019).

Apesar dos desafios, a IA oferece oportunidades significativas. A análise preditiva baseada em *big data* e *machine learning* pode otimizar a distribuição de recursos policiais, permitindo intervenções mais direcionadas e eficazes (Mandalapu et al., 2023). Barroca (2021), no seu estudo, indica que tecnologias de IA podem reduzir a criminalidade em até 30 a 40% e os tempos de resposta dos serviços de emergência em 20 a 35%. No entanto, a automação excessiva das decisões pode limitar a autonomia dos agentes no terreno, exigindo capacitação contínua e um quadro legal sólido (Moleirinho, 2021; Pedroso & Santos, 2024).

A falta de transparência e dificuldades de auditoria são desafios críticos, pois a fiscalização dos algoritmos é essencial para evitar decisões arbitrárias e garantir *accountability* (Olaoye & Egon, 2024; Pearson, Adey, & Jensen, 2024). Em resposta, a UE estabeleceu um regime jurídico harmonizado, reforçando a necessidade de supervisão e participação da sociedade na definição dos limites da tecnologia (Parlamento Europeu e Conselho da União Europeia, 2024).

Em suma, a literatura revela uma discrepância entre o otimismo em relação ao potencial da IA e a falta de estudos empíricos que comprovem a sua eficácia, reforçando a necessidade de avaliações rigorosas baseadas em evidências concretas (Meijer & Wessels, 2019). Enquanto alguns estudos apontam para o seu potencial na otimização de recursos e na antecipação de padrões criminais (Mandalapu et al., 2023; Olaoye & Egon, 2024), outros sublinham a falta de validação empírica e os riscos de enviesamento algorítmico e discriminação estrutural (Ferguson, 2020; Magalhães et al., 2024; Meijer & Wessels, 2019). Assim, enquanto a IA revoluciona a segurança pública, a sua aplicação eficaz depende da melhoria contínua dos modelos tecnológicos e da implementação de diretrizes éticas robustas (Floridi & Cowls, 2019). Apenas uma abordagem que combine inovação, ética e transparência permitirá consolidar a IA como uma ferramenta eficaz na prevenção da criminalidade e na construção de uma segurança pública mais eficiente.

5. CONCLUSÕES

O presente estudo procedeu a uma análise sistemática dos desafios e oportunidades decorrentes da implementação da IA no policiamento preditivo, com particular enfoque na sua aplicabilidade na análise e prevenção criminal. Através de uma revisão bibliográfica abrangente, examinou-se a evolução da IA e do policiamento preditivo, as suas aplicações práticas e os impactos éticos, legais, técnicos e operacionais resultantes da sua operacionalização. Esta investigação procurou apresentar uma perspetiva pormenorizada sobre as implicações da IA no contexto do policiamento e nas estratégias de segurança pública.

A análise desenvolvida, após uma conceptualização da IA e da sua evolução, evidenciou a premência de instrumentos inovadores no domínio do policiamento, face à crescente complexidade do fenómeno criminal. A IA tem vindo a revolucionar o policiamento preditivo, potenciando a análise de padrões criminais e a otimização na alocação de recursos. A sua adaptabilidade aos diversos paradigmas securitários demonstra a sua consonância com as diferentes escolas de pensamento, desde abordagens centradas na problemática social até modelos orientados para a vigilância e controlo. Não obstante, a sua implementação suscita questões prementes de natureza ética, legal, técnica e operacional, onde distintas correntes teóricas debatem o impacto da IA na prevenção criminal e na salvaguarda dos direitos fundamentais.

Em resposta à questão central de investigação – Quais são os desafios e oportunidades decorrentes da aplicação da Inteligência Artificial no policiamento preditivo? – verificou-se que a IA potencia significativamente a eficiência policial, possibilitando análises preditivas, identificação de padrões criminais e antecipação de ocorrências delituosas. Os principais benefícios identificados incluem uma otimização na distribuição de recursos, redução dos tempos de resposta e incremento da eficiência operacional. Os estudos analisados apontam para potenciais reduções na criminalidade na ordem dos 30% a 40%.

Todavia, identificaram-se desafios significativos, nomeadamente questões relacionadas com a privacidade, discriminação algorítmica e ausência de transparência, para além de constrangimentos técnicos associados à qualidade dos dados, robustez dos algoritmos e necessidade de supervisão humana. O estudo evidenciou que a interpretação criteriosa dos dados assume particular relevância na prevenção de decisões enviesadas que possam afetar desproporcionalmente determinados segmentos da população.

O Regulamento da IA da UE, publicado em 2024, estabelece requisitos rigorosos para sistemas classificados de risco elevado, como aqueles utilizados pelas forças de segurança no âmbito do policiamento preditivo, visando assegurar a proteção dos direitos fundamentais e a utilização ética da tecnologia. Contudo, este instrumento normativo exclui do seu âmbito de aplicação os sistemas desenvolvidos para fins militares, de defesa ou de segurança nacional, conceito que se reveste de particular ambiguidade no contexto português.

No panorama nacional, a implementação da IA no policiamento preditivo encontra-se ainda numa fase embrionária, com algumas forças e serviços de segurança a desenvolverem projetos-piloto e parcerias com instituições académicas e outras entidades. Embora Portugal tenha sancionado a aplicação destas tecnologias, advogando que restrições excessivas não devem comprometer a atuação policial, a sua operacionalização requer particular atenção, considerando a inexistência de uma entidade reguladora estabelecida à data da entrada em vigor das disposições relativas às práticas proibidas de IA e a ausência de um enquadramento jurídico preciso para o conceito de segurança nacional, suscetível de gerar ambiguidades na aplicação de sistemas de IA para fins de policiamento e análise preditiva.

Verificou-se que o estudo, embora compreensivo e abrangente, apresenta algumas limitações. A análise bibliográfica poderá não ter contemplado a totalidade da diversidade de perspetivas e estudos existentes sobre a temática.

Adicionalmente, a célere evolução da IA e as constantes alterações legislativas e tecnológicas condicionam qualquer análise a um momento temporal específico. A escassez de estudos de caso em Portugal dificultou uma análise mais aprofundada da realidade nacional, e a análise circunscrita a determinados exemplos de aplicação da IA poderá limitar a compreensão do seu impacto global em diferentes contextos policiais.

Para investigações futuras, propõe-se a realização de estudos de caso sobre a operacionalização da IA no policiamento em Portugal, incluindo a análise dos benefícios, desafios e implicações ético-jurídicas. Afigura-se fundamental que as investigações subsequentes se centrem igualmente na análise do impacto do Regulamento da IA nas práticas policiais e desenvolvam estudos sobre a perceção pública e a aceitação social do policiamento preditivo.

Este estudo contribui para o conhecimento científico através da sistematização dos desafios e oportunidades da IA no policiamento preditivo, considerando dimensões éticas, jurídicas e técnicas. Face à evolução tecnológica e à crescente preocupação com a segurança, evidencia-se a necessidade premente de regulamentação e supervisão para assegurar a confiança pública e a eficácia operacional.

Em conclusão, a implementação da IA deve pautar-se por princípios éticos e de responsabilidade, salvaguardando o respeito pelos direitos fundamentais, nomeadamente os direitos à privacidade e à proteção contra intromissões arbitrárias na vida pessoal e familiar. Esta tecnologia apresenta potencial para transformar significativamente o policiamento preditivo, otimizando a prevenção criminal. Contudo, o seu êxito dependerá da existência de um enquadramento normativo robusto e da adoção de boas práticas que assegurem o equilíbrio entre segurança, direitos individuais e valores democráticos. O futuro do policiamento não se alicerça exclusivamente na tecnologia, mas na construção de um modelo sustentável e legítimo que garanta uma utilização justa e eficiente da IA.

REFERÊNCIAS BIBLIOGRÁFICAS

Agência para a Modernização Administrativa (AMA). (2022). *Guia para uma inteligência artificial ética, transparente e responsável na administração pública* (Versão 1.1). https://digital.gov.pt/documentos/guia-para-uma-inteligencia-artificial-etica-transparente-e-responsavel-na-administracao-publica

Andrade, T. V. (2022). *O uso da inteligência artificial no policiamento preditivo* [Dissertação de Mestrado, Universidade do Minho]. Universidade do Minho.

Assembleia da República. (2008). *Lei n.º 53/2008, de 29 de agosto, que aprova a Lei de Segurança Interna, com alterações pelo Decreto-Lei n.º 99-A/2023, de 27 de outubro*. *Diário da República*, 1.ª série, n.º 167.

Assembleia da República. (2021). *Lei n.º 27/2021, de 17 de maio, que aprova a Carta Portuguesa de Direitos Humanos na Era Digital*. *Diário da República*, 1.ª série, n.º 95.

Bardin, L. (1997). *Análise de conteúdo*. Edições 70.

Barroca, J. G. (2021). Surveillance and predictive policing through AI. In Deloitte (Ed.), *Urban future with a purpose: 12 trends shaping the future of cities by 2030* (pp. 130-137). Deloitte Insights. https://living-in.eu/knowledge-base/urban-future-purpose-12-trends-shaping-future-cities

Baughman, S. B. (2020). How effective are police? The problem of clearance rates and criminal accountability. *Alabama Law Review, 72*(1), 47–130.

Bigo, D. (2002). Security and immigration: Toward a critique of the governmentality of unease. *Alternatives, 27*(1_suppl), 63–92. https://migrantsproject.eu/wp-content/uploads/2020/08/Bigo_Security-and-Immigration.pdf

Bigo, D., Isin, E., & Ruppert, E. (Eds.). (2019). *Data politics: Worlds, subjects, rights*. Routledge. https://doi.org/10.4324/9781315167305

Bossong, R., & Hegemann, H. (2018). The governance of internal security: Beyond functionalism and the finality of integration. In A. Ripoll Servent & F. Trauner (Eds.), *The Routledge handbook of justice and home affairs research* (pp. 19-29). Routledge.

Bostrom, N. (2014). *Superintelligence: Paths, dangers, strategies*. Oxford University Press.

Brantingham, P., Brantingham, P. J., & Taylor, W. (2005). Situational crime prevention as a key component in embedded crime prevention. *Canadian Journal of Criminology and Criminal Justice, 47*(2), 271–292.

Brayne, S. (2021). Dye in the cracks: The limits of legal frameworks governing police use of big data. *St. Louis University Law Journal, 65*(4), 823–836.

Buzan, B. (1998). *Security, the State, the "New World Order," and Beyond*. In R. D. Lipschutz (Ed.), On security (pp. 143–159). Columbia University Press.

Cardoso, L. (1981). *Defesa Nacional - Segurança Nacional*. *Nação e Defesa, 6*(17). Instituto da Defesa Nacional. http://hdl.handle.net/10400.26/3522

Comissão Europeia. (2019). *Aumentar a confiança numa inteligência artificial centrada no ser humano* (COM(2019) 168 final). Comissão Europeia.

Comissão Europeia. (2020). *Livro Branco sobre a inteligência artificial: Uma abordagem europeia virada para a excelência e a confiança* (COM(2020) 65 final). Comissão Europeia.

Conselho da Europa. (1950). *Convenção Europeia dos Direitos Humanos*. Concelho da Europa.

Europol. (2024). *AI and policing: The benefits and challenges of artificial intelligence for law enforcement*. Publications Office of the European Union. ISBN 978-92-95220-92-8. DOI: 10.2813/42230.

Executive Digest. (2025, 22 de janeiro). *Vigilância com IA pelas forças de segurança chega à UE em fevereiro – Portugal aprova uso livre da tecnologia*. Executive Digest. https://executivedigest.sapo.pt/noticias/vigilancia-com-ia-pelas-forcas-de-seguranca-chega-a-ue-em-fevereiro-portugal-aprova-uso-livre-da-tecnologia/.

Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. NYU Press.

Ferguson, A. G. (2020). Big data prosecution and Brady. *UCLA Law Review, 67*(1), 180–256.

Ferreira, J., João, P., & Martins, J. (2012). GIS for crime analysis: Geography for predictive models. T*he Electronic Journal Information Systems Evaluation, 15*(1), 36–49.

Floridi, L., & Cowls, J. (2019). A unified framework of five principles for AI in society. *Harvard Data Science Review*. https://doi.org/10.1162/99608f92.8cd550d1.

Fonseca, J. N. D. (2010). *O conceito de segurança nacional perspectivado para 2030*. Instituto Universitário Militar. http://hdl.handle.net/10400.26/12079.

Foucault, M. (2008). *Segurança, território, população: Curso dado no Collège de France (1977-1978)*. Martins Fontes.

Hermenegildo, R. S. (2013). *Autonomização, emergência e afirmação da segurança interna da União Europeia*. Nação e Defesa, 135, 153-171. http://hdl.handle.net/10400.26/14560

Hermenegildo, R. S. (2018). *A "segurança interna" da União Europeia: O caso da Guarda Costeira e de Fronteiras*. Proelium, VII(14), 147-182. https://run.unl.pt/bitstream/10362/61130/1/A_seguran_a_interna_da_Uni_o_Europeia.pdf

Inspeção-Geral dos Serviços de Justiça (IGSJ). (2025, 28 de janeiro). Regulamento de Inteligência Artificial. IGSJ. https://igsj.justica.gov.pt/Noticias-da-IGSJ/Regulamento-de-Inteligencia-Artificial

Magalhães, A. R. R., Crestani, A. C., Franco, L. C., et al. (2024). Inteligência artificial e manutenção da ordem pública: Impacto da proposta de Regulamento da IA no direito português [Relatório Final, Instituto Jurídico, Universidade de Coimbra].

Mandalapu, V., Elluri, L., Vyas, P., & Roy, N. (2023). Crime prediction using machine learning and deep learning: A systematic review and future directions. *IEEE Access, 11*, 60153-60170. https://ieeexplore.ieee.org/document/10151873.

Meijer, A., & Wessels, M. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration, 42*(12), 1031–1039. https://doi.org/10.1080/01900692.2019.1575664

Ministério da Ciência, Tecnologia e Ensino Superior. (2019). *AI Portugal 2030: An innovation and growth strategy to foster Artificial Intelligence in Portugal in the European context*. Ministério da Ciência, Tecnologia e Ensino Superior. https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v==BAAAAB+LCAAAAAAABACzMDQxAQC3h+yrBAAAAA==

Moleirinho, P. M. S. E. (2021). *Aplicação da Inteligência Artificial ao serviço da função policial* [Curso de Promoção a Oficial General, Instituto Universitário Militar]. Instituto Universitário Militar.

Moleirinho, P., Baraças, B., & Augusto, R. S. (2024). *Os modelos preditivos de segurança pública: A aplicação da inteligência artificial*. In T. Rodrigues & J. Estevens (Eds.), Preparar o futuro: A transição digital na segurança e defesa (pp. 201–226). Fronteira do Caos.

Nações Unidas. (1948). *Declaração Universal dos Direitos Humanos*. Assembleia Geral das Nações Unidas.

Olaoye, F., & Egon, A. (2024). Predictive policing and crime prevention. *Crime & Delinquency, 70*(4), 341–356.

Organização para a Segurança e Cooperação na Europa (OSCE). (2017). *OSCE Guidebook on Intelligence-Led Policing*. Transnational Threats Department: Strategic Police Matters Unit.

Parlamento Europeu e Conselho da União Europeia. (2016). Diretiva (UE) 2016/680, de 27 de abril 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, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. OJ L 119, p. 89–131. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016L0680

Parlamento Europeu e Conselho da União Europeia. (2024). *Regulamento (UE) 2024/1689: Regras harmonizadas em matéria de inteligência artificial*. Jornal Oficial da União Europeia, L de 12 de julho de 2024. http://data.europa.eu/eli/reg/2024/1689/oj

Pearson, E., Adey, P., & Jensen, R. B. (2024). Pred-Pol-Pov: Visibility, data flows, and the predictive policing of poverty. *Surveillance & Society, 22*(2), 120–137. https://doi.org/10.24908/ss.v22i2.15826

Pedroso, J., & Santos, A. (2024). Inteligência artificial e justiça criminal: Riscos e desafios. *Sociologia On Line, 35*, 134-155. https://revista.aps.pt/wp-content/uploads/2024/11/n35a06.pdf

Polícia Judiciária. (2021). *DARLENE*. https://www.policiajudiciaria.pt/projetos-financiados/darlene/.

Polícia Judiciária. (2021). *GRACE*. https://www.policiajudiciaria.pt/projetos-financiados/grace/

Polícia Judiciária. (2022). *STARLIGHT*. https://www.policiajudiciaria.pt/projetos-financiados/starlight/

Proença, L. (2023). Inteligência artificial na segurança: Um desafio ou uma inevitabilidade? In *88 Vozes sobre a IA: O que fica para a máquina e o que fica para o homem* (pp. 438–442). Editora Desafios Tecnológicos.

Público. (2025, 22 de janeiro). *Portugal defendeu e aprovou o uso livre da inteligência artificial pelas forças de segurança*. Público. https://www.publico.pt/2025/01/22/politica/noticia/portugal-defendeu-aprovou-uso-livre-inteligencia-artificial-forcas-seguranca-2119626

Ramos, A. D. (2023). A IA e a sua aplicação na investigação criminal: Contributo para a identificação de perfis na criminalidade organizada. *Anatomia do Crime, 17*(janeiro-junho), 159–168.

Ratcliffe, J. H. (2003). Intelligence-led policing. *Trends & Issues in Crime and Criminal Justice, 248*. Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi248

Ratcliffe, J. H. (2004). Crime mapping and the training needs of law enforcement. *European Journal on Criminal Policy and Research*, 10, 65–83. https://doi.org/10.1023/B:CRIM.0000037550.40559.1c

Rodrigues, A. M., Fidalgo, S., & Pais, A. (2022). AI and administration of criminal justice: Portuguese report. *Portuguese Criminal Policy and AI*.

Russell, S. J., & Norvig, P. (2016). *Artificial intelligence: A modern approach*. Pearson.

Telles, P. S. B. (2021). Inteligência artificial e polícia preditiva: limites e possibilidades. *Boletim Científico Escola Superior do Ministério Público da União, 57*, 247–263. https://escola.mpu.mp.br/publicacoescientificas/index.php/boletim/art article/view/613

TSF. (2019, 29 de março). Universidade de Évora e GNR de Setúbal usam inteligência artificial para reduzir acidentes. *TSF Notícias*. https://www.tsf.pt/sociedade/universidade-de-evora-e-gnr-de-setubal-usam-inteligencia-artificial-para-reduzir-acidentes-10738910.html/

U.S. Government Accountability Office (GAO). (2018). *Artificial Intelligence: Emerging Opportunities, Challenges, and Implications*. *GAO Reports*, i-94. https://www.gao.gov/assets/700/691536.pdf

Wæver, O. (1998). *Securitization and desecuritization*. In R. D. Lipschutz (Ed.), On security (pp. 46–86). Columbia University Press.

Walt, S. M. (1991). The renaissance of security studies. *International Studies Quarterly, 35*(2), 211–239.: http://ereserve.library.utah.edu/Annual/POLS/5690/Lobell/renaissance.pdf

Wuschke, K. E., Andresen, M. A., Brantingham, P. J., Rattenbury, C., & Richards, A. (2018). What do police do and where do they do it? *International Journal of Police Science & Management, 20*(1), 19–27. https://doi.org/10.1177/1461355717748973

Zenor, J. (2021). If you see something, say something: Can artificial intelligence have a duty to report dangerous behavior in the home? *Denver Law Review, 98*(4), 839–865.

ESTUDO 6 – VIDEOVIGILÂNCIA COM INTELIGÊNCIA ARTIFICIAL NA UNIÃO EUROPEIA: PERTINÊNCIA E ENQUADRAMENTO

VIDEO SURVEILLANCE WITH ARTIFICIAL INTELLIGENCE IN THE EUROPEAN UNION: RELEVANCE AND LEGAL FRAMEWORK

João Manuel Roxo Carreiro
Capitão GNR

RESUMO

O presente artigo investiga a conjuntura atual das tecnologias de videovigilância integradas com Inteligência Artificial (IA) na União Europeia (UE), com passagem pelos principais conceitos associados, abordagem sobre o papel crescente da IA nos sistemas de vigilância e reflexão sobre os limites éticos e legais da sua implementação, estabelecendo um foco quase transversal na tensão entre segurança pública e direitos fundamentais.

No desenvolvimento, proporciona-se uma análise bibliográfica integrada quanto às capacidades da IA aplicadas à videovigilância, as quais incluem verificação de identidade, prevenção criminal, deteção de armas, previsão de ocorrências, comportamento de grupo e seguimento de indivíduos. Posteriormente, exploram-se os desafios técnicos, os riscos do uso indevido dos dados e os entraves legais, com destaque para as disposições das regulações europeias, que impõem restrições a práticas automatizadas em espaços públicos. Por fim, são apresentados alguns aspetos sociais e legais dos Estados Unidos da América e da China no que respeita às aplicações de IA na videovigilância.

Conclui-se que, embora a IA associada a sistemas de videovigilância contemple benefícios evidentes para a segurança, a UE adota uma abordagem cautelosa e regulatória, diferenciando-se do modelo mais permissivo dos EUA e do autoritarismo digital chinês.

Palavras-chave: Videovigilância; Inteligência Artificial; União Europeia.

ABSTRACT

This article investigates the current landscape of video surveillance technologies integrated with Artificial Intelligence (AI) within the European Union (EU), covering key concepts, the growing role of AI in surveillance systems and a reflection on the ethical and legal boundaries of its implementation. A central focus is placed on the ongoing tension between public security and fundamental rights.

Its development presents an integrated literature review on the capabilities of AI applied to

video surveillance, which include identity verification, crime prevention, weapon detection, incident prediction, group behaviour analysis and individual tracking. It then addresses the technical challenges, risks of data misuse and legal barriers, highlighting the provisions of European regulations that impose restrictions on automated practices in public spaces. Lastly, it outlines selected social and legal aspects of AI use in video surveillance in the United States of America and China.

The conclusion highlights that, although AI in surveillance systems offers clear security advantages, the EU adopts a cautious and regulatory stance, distinguishing itself from the more permissive approach of the USA and the digital authoritarianism evident in China.

***Keywords**: Video Surveillance; Artificial Intelligence; European Union.*

1. INTRODUÇÃO

O artigo ora apresentado tem com o objetivo de definir e enquadrar os conceitos de vigilância, monitorização e Inteligência Artificial (IA), culminando com a análise ao panorama legal e à problemática inerente à implementação de sistemas de videovigilância com recursos de IA na União Europeia (UE).

A dualidade liberdade/segurança é responsável por um dos principais debates na era da informação, especialmente considerando o incremento nas utilidades e capacidades das tecnologias de vigilância e recolha de dados, como o reconhecimento facial ou as ações preditivas automatizadas. O potencial da IA originou ferramentas poderosas para a prevenção e deteção criminal, contribuindo para a segurança pública (Piton, 2024).

O presente artigo apresenta uma revisão sistemática de bibliografia associada às capacidades de IA identificadas por vários autores, na perspetiva securitária, fornecendo o panorama de utilidade real das mesmas, enquanto se pondera sobre os desafios tecnológicos dessa ascensão e sobre os constrangimentos da sua implementação.

Nesta senda, procura-se também explorar os aspetos éticos e de privacidade que advêm da utilização de sistemas de videovigilância e de IA, abordando o seu potencial negativo, as dificuldades quanto à responsabilização das ações automatizadas e a necessidade preponderante do respeito pelos direitos fundamentais, de proteção de dados e de privacidade dos cidadãos.

Após o enquadramento legal na UE, concretiza-se uma reflexão sumária sobre o enquadramento nos Estados Unidos da América (EUA) e na China,

conferindo um contributo de enriquecimento ao estudo e proporcionando termos de comparação ao nível externo.

Por fim, pretende-se que as conclusões deste trabalho sejam focadas, permitindo cumprir o principal propósito da investigação, através da resposta à seguinte pergunta de partida: qual a conjuntura atual da videovigilância com IA na UE?

2. ENQUADRAMENTO CONCEPTUAL

Compreendendo-se a abrangência do presente trabalho e por forma a garantir a compreensão conceptual e o funcionamento das temáticas da vigilância, monitorização, recolha de informações e potencial do uso de IA nesses sistemas, nos próximos subcapítulos, efetua-se a explanação e análise desses tópicos.

2.1. Vigilância e monitorização

O conceito de vigilância é complexo e multifacetado, abrangendo diversas práticas e tecnologias utilizadas para monitorizar indivíduos e grupos. A vigilância é definida como a atenção intencional, rotineira e sistemática a detalhes pessoais com o objetivo de controlo, gestão, influência ou proteção. Esta definição inclui tanto as ações dos sistemas de informações (*intelligence*), como das empresas que visam a descoberta e verificação de determinadas atividades. A sociedade de vigilância carateriza-se pela utilização generalizada de tecnologias de vigilância, que são amplamente aceites como necessárias por razões económicas ou de segurança (Wright et al., 2015).

Frois (2014), numa perspetiva de âmbito sociopolítico, aborda a relação entre as decisões de implementação de sistemas de videovigilância e os propósitos de controlo social, referindo que os contextos histórico e político de cada Estado influenciam o entendimento sobre o tipo de medidas a adotar para gerar proteção e segurança. No caso de estudo da autora, realça-se a subjetividade da situação da Polónia, que contraria a suposição de que países com histórico de repressão tendem a demonstrar uma resposta mais negativa face à videovigilância, sugerindo-se que a aceitação ou resistência à videovigilância e ao controlo social, pode ser influenciada por fatores mais complexos do que apenas o passado político (Frois, 2014).

Por sua vez, Lysova (2024) compreende a videovigilância através de duas abordagens teóricas principais: a sociedade de vigilância e o estado de segurança. A primeira, inspirada nas ideias de Foucault sobre disciplina, encara a

videovigilância como um instrumento para normalizar o comportamento e exercer poder disciplinar, sendo as câmaras de circuitos fechados de televisão (CCTV), nessa perspetiva, usadas para recolher, armazenar e estruturar informações sobre os indivíduos, permitindo rastrear desvios do comportamento padrão. A autora argumenta que a presença de videovigilância, sinalizada de forma visível, tem como objetivo incutir a noção de que as pessoas estão a ser vigiadas, levando-as a comportarem-se de forma normalizada e conferindo às autoridades a possibilidade de acompanharem indivíduos ou grupos específicos, antecipando a ocorrência de crimes (Lysova, 2024).

A abordagem do estado de segurança considera que a sociedade vive num clima de emergência permanente, onde a vigilância é justificada pela necessidade de proteger a população "comum" da criminalidade grave e do terrorismo, sendo uma perspetiva que pode promover a segregação social e espacial, com as áreas mais seguras a serem fortificadas e as zonas potencialmente mais perigosas a serem marginalizadas. Segundo a autora, ambas as abordagens reconhecem que a videovigilância é uma forma de poder assimétrico, onde o observador permanece invisível e a sua identidade é preservada, e onde os sujeitos da vigilância têm um conhecimento limitado sobre quem os está a observar (Lysova, 2024).

Quanto à sua aplicabilidade, Wright *et al.* (2015) afirma que os sistemas de vigilância podem ser implementados para prevenção e proteção de cidadãos contra a criminalidade, monitorização de fronteiras e salvaguarda de interesses nacionais. Nas comunidades, podem empregar-se meios de videovigilância para aumentar o sentimento de segurança ou identificar problemas locais. Em contrapartida, os autores referem também os possíveis efeitos negativos provocados, incluindo a erosão da confiança e coesão sociais, podendo constituir um desafio à liberdade de ação, influenciando a forma como os indivíduos se movem, associam, pensam e participam nas atividades públicas (Wright et al., 2015).

No âmbito da segurança pública, Miranda et al. (2023) aponta que as atividades de recolha de informação são fulcrais para a prevenção de delitos e desordens públicas. O desenvolvimento destas áreas, onde se inclui a videovigilância, representa um desafio e uma necessidade, que exige o envolvimento dos municípios, que fazem parte do sistema de segurança pública, dos órgãos de polícia e de outros profissionais especializados, utilizando os sistemas de gestão de informações apropriados e o conhecimento para o planeamento e implementação de ações preventivas e repressivas contra a criminalidade (Miranda et al., 2023).

Confere-se o exemplo nacional (que, nos últimos anos se alargou a outras cidades, como Lisboa, Porto, Faro e Fátima), em respeito ao sistema de videovigilância na cidade da Amadora, implementado a partir de 2017, que consiste numa rede de câmaras de segurança espalhadas pelo concelho, geridas pela PSP, que operam 24 horas por dia, sem captação de som. O projeto inicial, proposto em 2008, foi reformulado e adaptado à legislação vigente, após parecer negativo da Comissão Nacional de Proteção de Dados, contanto o concelho da Amadora com 141 câmaras instaladas (dados de 2023). A sua aplicação teve como objetivo principal a redução da criminalidade, através da dissuasão e do apoio à monitorização de ocorrências por parte das forças de segurança. Aparentemente, atesta-se a eficácia da medida pelo facto de se ter registado uma redução de 60% na criminalidade violenta e grave, entre os anos de 2017 e 2022 (Lusa, 2023).

2.2. Aplicações da Inteligência Artificial à videovigilância

A IA é uma área das ciências da computação que procura criar sistemas capazes de realizar tarefas que, tradicionalmente, requeriam ação ou processamento humano, onde se inclui a utilização de raciocínio lógico, aprendizagem (*machine-learning*), reconhecimento de padrões e tomada de decisões. A IA difere da mera análise de dados, por utilizar algoritmos avançados, grandes volumes de dados e poder computacional para simular, ou superar, as capacidades cognitivas humanas em diversos contextos (Roser, 2022).

No contexto da videovigilância, mesmo com a inserção dos mecanismos de alerta (*flagging*) que atualmente já integram a maioria dos sistemas de recolha de imagem (e. g., criar destaques consoante se detete movimento), tipicamente, a análise de dados diferenciada continua a carecer do elemento humano para ser bem-sucedida. A IA surge na videovigilância com um potencial muito acrescido no que respeita ao tipo de dados que consegue recolher, tratar e analisar (Abba et al., 2024).

Com base na pesquisa bibliográfica efetuada, elaborou-se o Quadro 1, que reúne as capacidades mais relevantes que os vários autores identificam para a integração da IA no aumento das funcionalidades e na melhoria da qualidade da monitorização de segurança, através de recursos de recolha de imagem, como as câmaras de videovigilância.

Tabela 1 – Capacidades de IA com aplicação à videovigilância, identificadas por autor

		Autor					
		Fontes *et al.* (2022)	Roser (2022)	Abba *et al.* (2024)	Irene *et al.* (2024)	Pfau (2024)	Berardini *et al.* (2025)
Capacidade	Verificação de identidade	x	x		x	x	
	Prevenção criminal	x	x	x			x
	Deteção de armas		x	x			x
	Previsão de ocorrências	x	x			x	
	Comportamento de grupo			x	x		
	Seguimento de indivíduos	x		x	x	x	

No seguimento das capacidades de IA supra identificadas, todas elas relacionadas com o setor da segurança, destaca-se que a "verificação de identidade" é referida por quatro autores, que descrevem a sua abrangência como a possibilidade de reconhecer pessoas em tempo real através do rosto (Roser, 2022; Pfau, 2024), comparando expressões faciais com as bases de dados existentes, para encontrar desaparecidos (Fontes et al., 2022), ou procurar correspondências através de toda a linguagem corporal ou tipo de roupa utilizada pelo indivíduo (Irene et al., 2024).

Os fins de "prevenção criminal" são mencionados por quatro autores, que apontam a capacidade da IA para identificar suspeitos, criminosos ou terroristas conhecidos (Fontes et al., 2022), realçar comportamentos suspeitos de um indivíduo (Roser, 2022) ou contribuir para o controlo de tráfego e para a prevenção de crimes nos espaços públicos (Abba et al., 2024).

A "deteção de armas", enquanto elemento de extrema relevância para a condução da atividade policial segura, é referida por três autores, que indicam técnicas de aprendizagem profunda (*deep-learning*) para a deteção e monitorização de armas (Abba et al., 2024), bem como, o desenvolvimento de abordagens automáticas (e. g., através do modelo *You Only Look Once*) para encontrar armas ou outros objetos de pequenas dimensões, em tempo real, mesmo em ambientes com recursos limitados, como espaços públicos condicionados ou com maior densidade de pessoas (Berardini et al., 2025).

Quanto à "previsão de ocorrências", três autores referem-na enquanto contributo para o policiamento preditivo, justificando com a possibilidade da IA para distinguir comportamentos humanos padrão de condutas erráticas (Fontes et

al., 2022), para identificar potenciais situações de risco antes de ocorrerem (Roser, 2022) ou para analisar dados pessoais em larga escala, conseguindo prever, dentro de determinado contexto, o que agrada ou desagrada o indivíduo, resultando em possíveis reações do mesmo face aos estímulos a que está exposto (Pfau, 2024).

Dois autores aludem ao "comportamento de grupo", enquanto capacidade de leitura e interpretação das movimentações de um aglomerado de pessoas (Abba et al., 2024) ou para análise do comportamento de uma multidão, e. g., através da contagem de pessoas (*crowd couting)* para cálculo de métricas sociais (Irene et al., 2022).

Por fim, o "seguimento de indivíduos" é apontado por quatro autores, que o descrevem como a possibilidade para procura e acompanhamento de pessoas em ambientes congestionados (Abba et al., 2024), pesquisa de pessoas por vídeo (Irene et al., 2022) ou deteção de movimentos de indivíduos selecionados (Pfau, 2022).

Tendo sido referidas as capacidades da IA associadas à segurança pública que se consideram mais determinantes, importa também indicar os principais constrangimentos à sua aplicação, que englobam: a necessidade de recursos computacionais mais avançados e com capacidade superior, aumentando os custos de aquisição e manutenção dos sistemas (Pfau, 2024); para efeitos de prevenção criminal, é necessário começar pela introdução na IA de bases de dados sintéticas, o que pode reduzir a sua eficácia real e condicionar a implementação prática (Berardini et al., 2025); complexidade da análise de vídeo ou imagens com variações subtis (e. g., para distinção de indivíduos sem a face visível, com estatura e roupas semelhantes) (Irene et al., 2022); a dificuldade de análise pormenorizada em ambientes com elevada concentração de pessoas (Berardini et al., 2025); e a possibilidade de utilização abusiva dos dados recolhidos e analisados para fins não previstos (Roser, 2022).

3. ASPETOS ÉTICOS E DE PRIVACIDADE

Apesar dos possíveis benefícios da videovigilância para a segurança pública, previamente salientados pelos diversos autores, subsistem algumas dimensões de cariz ético e de violação dos direitos fundamentais dos cidadãos que podem advir da sua utilização. Note-se que, no passado, em linha com a proteção do direito à vida privada, já previsto na Convenção Europeia dos Direitos Humanos previamente à Carta dos Direitos Fundamentais da UE, a Assembleia Parlamentar do Conselho da Europa (APCE) impôs limites ao uso de tecnologias de vigilância, indicando o

seu uso apenas como medida excecional e proporcional, quando as alternativas fossem inadequadas. Apesar desse entendimento, com o avanço da tecnologia e o aumento da sensação de insegurança, a aceitação pública da videovigilância como ferramenta útil para prevenção e deteção de crimes foi-se ampliando, suportada por casos emblemáticos em que a eficácia desses sistemas foi comprovada, como nos atentados de Londres, em 2005 (APCE, 2008).

Posteriormente, com o aumento das tecnologias associadas à videovigilância, entendeu-se que a sua adoção intensiva, associada à recolha massiva de dados (sobretudo, os biométricos), pode originar um fenómeno conhecido como "efeito arrepiante" (*chilling effect*), no qual as pessoas mudam os seus comportamentos por se sentirem constantemente observadas. Este cenário é especialmente preocupante quando ocorre em espaços destinados à expressão livre e à associação, como praças e locais de protesto, em que a proteção das liberdades e garantias dos cidadãos devem ser plenamente respeitadas (AEPD, 2013; CEPD, 2020).

O estudo de Finn e Wright (2016), remetendo-se ao setor da vigilância através de câmaras incorporadas em aeronaves não tripuladas (*drones*), cuja utilização se propagou nas forças de segurança e militares, levanta questões éticas e de privacidade significativas devido às suas elevadas capacidades e aplicações, salientando o facto desses equipamentos, quando dotados de câmaras, capturarem imagens de pessoas, intencionalmente ou não, independentemente do seu consentimento, podendo revelar informações sobre a sua identidade, localização, comportamento ou outras características do foro pessoal (Finn e Wright, 2016).

Ao encontro das preocupações manifestadas no parágrafo anterior, os autores referem o impacto negativo que a simples presença de *drones* pode provocar no comportamento das pessoas, referindo igualmente o "efeito arrepiante", motivado pelo receio que sentem por estarem a ser observadas. Argumenta-se ainda que o uso desse tipo de dispositivos pode levar a que os grupos marginalizados sejam alvo de maior vigilância, correndo-se o risco de a tecnologia contribuir para exacerbar tensões sociopolíticas já existentes (Finn e Wright, 2016).

Outro estudo mais recente, que aborda os aspetos de segurança, ética e privacidade relacionados com os sistemas de verificação de identidade através de reconhecimento facial, confirma algumas questões previamente levantadas, salientando os seguintes pontos: desrespeito pela privacidade (pendência para a vertente da segurança na ponderação com o direito à privacidade), considerando que podem ser recolhidos dados não autorizados, existir falta de conhecimento

ou consentimento, e utilização indevida de dados, para fins diferentes do objetivo original; resignação digital, enquanto sentimento de futilidade originado pelo pensamento de que a falta de liberdade ou privacidade é o preço a pagar pela segurança; discriminação, revelando preocupação com a forma como os algoritmos de IA são treinados, através de bases de dados extensas, mas que nem sempre contém a devida representatividade de cidadãos, podendo originar imprecisões na identificação de pessoas de certas origens raciais e étnicas, aumentando o preconceito; erosão da confiança, no sentido em que a vigilância extensiva pode levar a uma perda da ligação entre o governo e a população, quando os motivos e as necessidades não forem claros (Choung, 2024).

Outros riscos da videovigilância envolvem a falta de transparência sobre como os dados são recolhidos, armazenados e analisados. Na maioria dos casos, os indivíduos monitorizados não têm conhecimento ou controle sobre como serão tratadas as suas informações pessoais, o que, conjugado com a ausência de regulamentações claras e abrangentes, pode abrir espaço a utilizações abusivas de dados, e. g., para vigilância em massa e repressão política (Pfau, 2024).

Para mitigar o potencial de abuso e garantir a conformidade legal, a UE regulamentou no sentido de exigir a adoção de medidas técnicas e organizacionais adequadas, onde se incluem a encriptação de imagens, a limitação de acesso a dados sensíveis e a definição de políticas claras para o armazenamento e a eliminação de informações adquiridas por meio dos sistemas de vigilância (AEPD, 2013; CEPD, 2020).

Em complemento, Pfau (2024) indica que, para mitigar os riscos, é fundamental adotar medidas rigorosas para proteção dos direitos fundamentais e da privacidade, como a aplicação de criptografia avançada e anonimização de dados, além de ter de se assegurar, sobretudo através de regulamentação e transparência, que os sistemas que utilizem capacidades de IA também respeitem princípios éticos e direitos humanos (Pfau, 2024).

Face a este último propósito, na perspetiva da aplicação da IA à investigação criminal, constata-se que "*são diversos os problemas que se colocam com o uso de IA no âmbito do Direito Penal*" (Ramos, 2023, p. 159), destacando o autor a dificuldade de enquadramento da criminalização de ações efetuadas por *software* informático, levantando-se principalmente questões quanto à entidade verdadeiramente responsável pelos atos praticados – o programa, o programador ou o utilizador? – e quando às possíveis penas a aplicar para reparar o mal provocado – erradicação do *software* e/ou culpabilização do criador? (Ramos, 2023).

4. ENQUADRAMENTO

Aborda-se na presente seção a contextualização legal da vigilância, monitorização e IA, numa perspetiva conceptual e evolutiva, no prisma da UE e, posteriormente, de forma sumária, é elaborado o panorama legal e social sobre as mesmas temáticas nos EUA e na China, apresentando-se dois enquadramentos bastante díspares, para consideração e comparação.

4.1. Na União Europeia

A UE apresenta-se, na esfera mundial, como uma organização internacional de primeira linha, de sociedade evoluída e que prima pela afincada prossecução dos direitos, liberdades e garantias dos cidadãos que residem ou se encontram no seu espaço territorial. Em relação à privacidade e segurança de dados, enquanto preocupações intrínsecas às matérias da vigilância e monitorização, constata-se que a UE desde longa data as considerou no seu vocabulário e na sua agenda, mantendo uma visão de interesse e integração sobre esses conteúdos.

No seu quadro legal e regulamentar, identificam-se os seguintes documentos basilares, por ordem cronológica, que sustentam a visão atual da UE sobre os tópicos da vigilância e monitorização:

- Resolução n.º 1604, de 25 de janeiro de 2008, da APCE, que discute a videovigilância em espaços públicos, reconhecendo a sua crescente implementação e eficácia na prevenção criminal, enquanto espelha a preocupação com potenciais violações de direitos humanos, nomeadamente à privacidade, defendendo uma regulamentação legal estrita, que equilibre a segurança pública com as garantias individuais;
- Diretriz do Supervisor Europeu de Proteção de Dados (SEPD) sobre a videovigilância, de 17 de março de 2010, que oferece orientações práticas sobre o planeamento, implementação e funcionamento de sistemas de videovigilância, focando a minimização do impacto na privacidade e o respeito pelos direitos fundamentais;
- Folheto do SEPD acerca da videovigilância na administração da UE, de 16 de dezembro de 2013, que aconselha o uso responsável de videovigilância nas instituições da EU, destacando a necessidade de equilibrar a segurança e o direito à privacidade;
- Regulamento n.º 679/2016 (Regulamento Geral para a Proteção de Dados – RGPD), de 04 de maio de 2016, com efeitos a partir de 25 de

maio de 2018, substituindo a desatualizada Diretiva n.º 95/46/CE, de 24 de outubro de 1995, do Parlamento Europeu e do Conselho da UE (PECUE), relativa ao tratamento e circulação de dados pessoais de pessoas singulares;

- Diretriz n.º 3/2019 (Versão 2.0), do Comité Europeu para a Proteção de Dados (CEPD), sobre o processamento de dados pessoais através de dispositivos de vídeo, com adoção a partir de 29 de janeiro de 2020, que representa um guia abrangente sobre a legalidade, à luz do RGPD, do processamento de dados (incluindo os biométricos), a sua divulgação e o interesse público.

No conceito da UE, a videovigilância é reconhecida como uma ferramenta poderosa para enfrentar questões de segurança. No entanto, o seu uso deve ser cuidadosamente ponderado devido ao possível impacto nos direitos fundamentais. O n.º 1 do artigo 8.º da Carta dos Direitos Fundamentais da UE e o n.º 1 do artigo 16.º do Tratado sobre o Funcionamento da UE, garantem a todas as pessoas o direito à proteção dos seus dados pessoais, incluindo os captados por sistemas de videovigilância (PECUE, 2012 e 2016b).

Historicamente, embora a UE elaborasse esclarecimentos e fornecesse instruções sobre a temática da proteção de dados, ocorriam variações significativas na implementação de legislações relacionadas à videovigilância entre os Estados-Membros, não existindo uma estrutura unificada para a proteção de dados. Destaca-se que alguns países impunham restrições mais rigorosas sobre o uso de tecnologias biométricas, enquanto outros adotavam normas mais flexíveis, e. g., para aplicações comerciais (APCE, 2008; AEPD, 2013). Esta disparidade reforçou a importância de diretrizes claras e precisas, como as elaboradas pelo Comité Europeu para a Proteção de Dados (CEPD), previsto e criado pelo RGPD, que atua enquanto organismo independente da UE, para desenvolver e assegurar a aplicação de orientações específicas para garantir uma abordagem coerente quanto à recolha e tratamento de dados eletrónicos no espaço da UE (CEPD, 2020).

Nesse sentido, acompanhando a crescente implementação de sistemas de videovigilância, foi igualmente necessário estabelecer normas claras para proteger os direitos fundamentais dos cidadãos, constituindo-se o RGPD, presentemente, como o principal instrumento legal da UE para regular a coleta e o tratamento de dados pessoais, incluindo os obtidos por dispositivos de captação de imagens (CEPD, 2020).

O RGPD surgiu precisamente com o intuito de modernizar e harmonizar a proteção dos direitos e liberdades das pessoas singulares no que respeita ao tratamento de dados pessoais, resolvendo as disparidades na aplicação da anterior Diretiva sobre a matéria, para assegurar um quadro de proteção de dados sólido e coerente, apoiado pela aplicação rigorosa das regras. A Diretiva, embora já estabelecesse princípios importantes, não conseguia evitar a fragmentação da aplicação da proteção de dados, provocando insegurança jurídica e perceção pública de riscos significativos para a proteção das pessoas, especialmente no contexto das atividades eletrónicas e no ciberespaço. Por outro lado, o RGPD estabelece um quadro geral para a proteção de dados, procurando assegurar aos cidadãos o direito à informação, direito de acesso, direito à retificação, direito ao apagamento ("esquecimento"), direito à limitação do tratamento, direito à portabilidade dos dados, direito de oposição e direito a não ser sujeito a decisões baseadas exclusivamente no tratamento automatizado (PECUE, 2016a).

A finalidade específica e a proporcionalidade, relativas ao tratamento de dados, já no passado mereciam especial atenção. A título de exemplo, câmaras instaladas em espaços públicos devem ser justificadas de forma clara e com motivos concretos, tais como, a prevenção criminal ou a proteção de bens. Não obstante a argumentação plausível, o uso de tecnologias avançadas que permitam reconhecimento facial ou a extração de dados pessoais através da leitura das imagens, requer avaliações de impacto rigorosas, considerando o potencial de violação dos direitos fundamentais (APCE, 2008; AEPD, 2013). A Autoridade Europeia para a Proteção de Dados (AEPD) alertou ainda que "(…) *a IA pode contribuir para desenvolvimentos sem precedentes* (…)", apresentando riscos muito elevados para a intrusão não democrática nas vidas privadas da população (Piton, 2024, p. 86).

No RGPD, as imagens captadas por câmaras de videovigilância são consideradas dados pessoais, uma vez que permitem identificar uma pessoa de forma direta ou indireta. Assim, o tratamento desses dados deve respeitar princípios, acautelar e reduzir impactos, e assegurar que os titulares tenham acesso às suas informações e possam exercer direitos, como a retificação ou o pedido de exclusão dos conteúdos que lhes dizem respeito (CEPD, 2020).

Assim, o RGPD estabelece uma série de princípios fundamentais para a recolha e tratamento de dados pessoais aplicáveis à videovigilância (PECUE, 2016a):

- Licitude, lealdade e transparência – Os titulares dos dados devem ser informados sobre a operação de tratamento e as finalidades a que se destinam;
- Limitação das finalidades – Os dados devem ser recolhidos para finalidades específicas, explícitas e legítimas, não podendo posteriormente ser analisados de forma incompatível com o que fora previsto;
- Minimização de dados – Os dados recolhidos devem ser necessários, adequados e pertinentes, evitando a sua recolha massiva ou excessiva;
- Limitação da conservação – Os dados devem ser conservados apenas durante o período necessário para as finalidades do seu tratamento;
- Integridade e confidencialidade – Os dados devem ser tratados de forma a garantir a sua segurança, incluindo a proteção contra o acesso ou tratamento não autorizado ou ilícito, a perda, destruição ou danificação acidental;
- Tratamento de dados sensíveis – Por poderem implicar riscos significativos para os direitos e liberdades fundamentais, estão previstos requisitos mais rigorosos de proteção face ao tratamento de categorias especiais de dados pessoais, onde se incluem os que possam revelar origem racial ou étnica, opiniões políticas, convicções religiosas ou filosóficas, filiação sindical, dados genéticos e dados relativos a saúde. Note-se que, à luz do RGPD, o tratamento de fotografias não se encontra aqui abrangido, por integrar a definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular. Salvo consentimento explícito do titular ou nos termos das restantes exceções previstas no n.º 2 do artigo 9.º, o RGPD proíbe o tratamento de dados sensíveis.

Para salvaguarda desses direitos, outro aspeto crucial é a transparência na utilização pública dos meios de videovigilância, exigindo-se que os indivíduos sejam informados sobre a presença desses sistemas (direito de informação) e os objetivos da sua utilização. Geralmente, tal deverá implicar a instalação de placas informativas e avisos detalhados, onde constem as políticas de privacidade aplicáveis aos dados recolhidos. Desta forma, para mitigar os riscos de abuso e garantir a conformidade legal, o RGPD exige a adoção de medidas técnicas e organizacionais

adequadas, onde se inclui a encriptação de imagens, a limitação de acesso a dados sensíveis e a definição de políticas claras para o armazenamento ou eliminação de informações (CEPD, 2020). Destarte, o RGPD prevê que se estabeleçam disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras previstas ao cumprimento de obrigações legais para o exercício de funções de interesse público (PECUE, 2016a).

No seguimento, é digno de menção que o artigo 23.º do RGPD contempla a possibilidade dos Estados-Membros poderem limitar, por medida legislativa, o alcance das obrigações previstas, desde que estritamente necessário e mantendo o respeito pela essência dos direitos e liberdades fundamentais, visando a prossecução dos seguintes objetivos principais: segurança e a defesa do Estado, segurança pública e a "*prevenção, investigação, deteção ou repressão de infrações penais (…), incluindo a salvaguarda e a prevenção de ameaças à segurança pública*" (PECUE, 2016a). Perante o enquadramento apresentado, as Forças e Serviços de Segurança (FSS) podem, para efeitos de prevenção e investigação criminal, aceder, visualizar e tratar os conteúdos de vídeo ou imagens recolhidas através de sistemas de videovigilância, permanecendo, no entanto, condicionadas à integração de recursos de análise com IA (e. g., reconhecimento facial) pela afirmação de que, mesmo nas circunstâncias elencadas, deve continuar a haver conformidade com a "essência" dos direitos fundamentais.

Nesta senda, no contexto do presente trabalho, importa também perceber a visão da UE, no que respeita à utilização das capacidades de videovigilância, quando potenciadas por *software* de IA. Se até à presente data existia uma certa ambiguidade nessa matéria, derivada da complexidade da identificação e reconhecimento do que realmente é a IA, a par do potencial do seu emprego, a partir de 2 de fevereiro de 2025 entram em vigor os capítulos I e II do Regulamento n.º 1689/2024 – Regulamento da IA, de 13 de junho de 2024, do PECUE, aplicando-se na sua plenitude, a partir de 2 de agosto de 2026.

Este novo normativo, que cria regras harmonizadas em matéria de uso da IA na UE, distingue "sistema de IA" por ser dotado da capacidade principal de conseguir fazer inferências, referindo-se ao processo de obtenção de resultados (e. g., previsões, conteúdos, recomendações ou decisões) que possam influenciar ambientes físicos e virtuais (PECUE, 2024).

Na parte que releva para as aplicações relativas à videovigilância, nos termos do n.º 1 do artigo 5.º do Regulamento da IA, são definidas entre as práticas proibidas (PECUE, 2024):

- al. c) – sistemas para avaliação ou classificação de pessoas ou grupos, com base no seu comportamento social ou em caraterísticas pessoais (impedimento do "crédito social");
- al. d) – sistemas para avaliação de risco de pessoas singulares a fim de avaliar ou prever a probabilidade de cometerem uma infração penal, com base exclusivamente na avaliação de perfis ou de traços (limitação ao "policiamento preditivo");
- al. e) e h) – sistemas que criem ou expandam bases de dados de reconhecimento facial através da recolha aleatória de imagens faciais a partir de CCTV, ou sistemas de identificação biométrica (e. g., comportamento, expressões e emoções) à distância, em tempo real e em espaços públicos, salvo em determinados casos de prevenção criminal, para fazer face a uma ameaça real e atual, ou real e previsível de um ataque terrorista;
- al. g) – sistemas de categorização biométrica para classificação de pessoas, com exceção de rotulagens ou filtragens de conjuntos de dados biométricos legalmente adquiridos, que permitam deduzir ou inferir a sua raça, opiniões políticas, filiação sindical, convicções religiosas ou filosóficas, vida ou orientação sexual.

O Regulamento da IA categoriza os sistemas de IA com base no risco que representam para a restrição de direitos fundamentais, prevendo particularidades específicas para os sistemas de IA de risco elevado, conforme disposto na Secção I, onde se inserem medidas de supervisão humana, documentação técnica, manutenção de registos, componente de cibersegurança e um sistema de gestão de qualidade por parte dos fornecedores desses serviços (PECUE, 2024).

Apesar disso, verifica-se que é conferida possibilidade para implementação de IA com menos restrições nos setores da segurança interna e externa, dado que o artigo 2.º refere que o Regulamento não afeta as competências dos Estados-Membros em matéria de segurança nacional, bem como, para finalidades militares ou de defesa (PECUE, 2024).

4.2. Nos Estados Unidos da América

Nos EUA, o documento basilar para a proteção de dados ainda é a Lei de Privacidade (*The Privacy Act*), de 1974, que regula a forma como as agências federais podem recolher e utilizar dados pessoais nos seus sistemas de registo, proibindo-se

a sua divulgação sem o consentimento expresso do titular, salvaguardadas algumas exceções (e. g., para fins estatísticos oficiais do governo). No entanto, ao contrário do que ocorre na UE, que elaborou diretrizes e regulou a proteção de dados (RGPD) e o uso de IA (Regulamento da IA) aplicáveis a todos os Estados-Membros, no caso dos EUA, existe uma abordagem mais fragmentada, com regulamentos específicos para diferentes setores e tipos de dados (Murray, 2023).

A ausência de legislação federal abrangente contribui para as disparidades entre Estados. Observe-se que, em cidades como São Francisco, São Diego, Oakland e Portland, os municípios foram proibidos de utilizar tecnologias de videovigilância com reconhecimento facial, enquanto noutras, como Detroit, o seu uso é permitido, embora restrito às FSS (Sahin, 2020). Importa salientar que, em 2018, a Califórnia aprovou a sua Lei de Privacidade do Consumidor (*Consumer Privacy Act*), atualizada dois anos depois com a Lei de Direitos de Privacidade (*Privacy Rights Act*), comparando-se o seu alcance ao do RGPD europeu (Murray, 2023).

Depois dos atentados de 11 de setembro de 2001, viveu-se nos EUA uma maior tolerância à restrição de certos direitos e liberdades individuais, alegando a eficácia das medidas de vigilância na prevenção e na repressão da criminalidade relacionada com o terrorismo, o que levou à aprovação do Ato Patriota (*USA Patriot Act*), em 24 de outubro do mesmo ano, passando a permitir-se, entre outras medidas, a videovigilância de pessoas que pudessem ter relação com o terrorismo, sem que fosse preciso qualquer autorização prévia da justiça (Piton, 2024).

Apesar disso, em 2020, com o emergir da contestação social em torno do racismo e da violência policial, algumas gigantes tecnológicas dos EUA, como a IBM, a Microsoft e a Amazon, suspenderam a venda de sistemas de reconhecimento facial para o meio policial, aguardando a aprovação de leis federais que protejam os direitos humanos (Sahin, 2020).

Quanto ao desenvolvimento e utilização de IA, a política dos EUA é moldada pelas prioridades de competitividade económica e liderança tecnológica, definindo-se pela orientação para o liberalismo do mercado e uma abordagem mais *laissez-faire* à regulamentação.

Simultaneamente, o tema da responsabilidade governamental tem sido amplamente debatido, sugerindo que o foco futuro dos EUA pode começar a incidir numa estratégia proativa para lidar com os desafios legais e as obrigações levantadas pelo uso dos sistemas de IA, esclarecendo o papel do Estado e os limites a estabelecer para fomentar o seu impacto positivo na sociedade, reduzindo os seus efeitos negativos (Wang et al., 2025).

4.3. Na China

A China encontra-se na vanguarda do desenvolvimento, uso e exportação de sistemas de vigilância com IA, devendo-se esse avanço, em parte, ao plano de Pequim para proporcionar a supremacia tecnológica a empresas como a Huawei, Hikvision e Dahua, que têm desenvolvido tecnologias para videovigilância de larga escala, com base em recursos de IA. As suas capacidades são potenciadas pelos produtos da SenseTime, Megvii e CloudWalk, *startups* líderes globais em tecnologias de reconhecimento facial. Por outro lado, a China também exporta estas tecnologias para vários países, incluindo o Uganda e o Zimbabué, com propósitos de controlo de fronteiras e vigilância em massa, recolhendo dados que permitem refinar os seus próprios algoritmos de reconhecimento facial para diferentes raças e etnias (Sahin, 2020).

Neste contexto, Piton (2024) destaca que a Huawei, em parceria com o governo, desenvolveu o projeto "Cidade Segura", que consiste na implementação de tecnologia de videovigilância em tempo real, para deteção e reconhecimento de pessoas, veículos ou objetos, conseguindo extrair dados de género, idade ou tipo de roupa. No seguimento, instaurou-se ainda um sistema de "crédito social", que representa um processo de avaliação de comportamento social, classificação e atribuição de uma pontuação, com fundamento na análise automatizada (algorítmica) dos dados recolhidos, culminando com o impacto em vários aspetos da vida quotidiana dos cidadãos observados, tanto para a atribuição de privilégios (e. g., melhores taxas de juro e acesso facilitado a habitação social) como para a aplicação de penalidades (e. g., perder acesso a empréstimos, dificuldade na obtenção de vistos, na entrada em eventos públicos e na aquisição de serviços de educação ou saúde) (Piton, 2024).

A China é o país do mundo com maior número de câmaras na via pública, per capita, tendo o uso extensivo de videovigilância com IA gerado críticas internacionais, com especial incidência na região de Xinjiang, onde é utilizada para reprimir elementos dos grupos étnicos Uigures e Cazaques. A esse propósito, a Huawei, líder na exportação de meios de vigilância com AI, foi acusada de desenvolver um sistema de câmaras com reconhecimento facial que identifica pessoas de minoria muçulmana, para alerta às autoridades (Wang et al., 2025).

As empresas chinesas do setor, têm inclusivamente procurado influenciar organismos internacionais, como a *International Telecommunication Union*, para a aceitação e expansão das aplicações de vigilância com IA, caraterizando-se o

país pela ausência de leis de privacidade e proteção de dados rigorosas, por uma forte participação governamental no desenvolvimento e produção de meios, e por um aparente grau de aceitação social dessas práticas. Independentemente da sua intenção na promoção do autoritarismo digital, a China está a aplicar e fornecer mecanismos para controlo social sem precedentes em todo o mundo (Sahin, 2020).

5. CONCLUSÕES

A videovigilância desempenha um papel crucial na sociedade contemporânea, oferecendo soluções eficazes para os desafios de segurança pública, apenas manchadas pelo seu igual potencial para atropelo aos direitos fundamentais. Os instrumentos legais europeus têm fornecido um arcabouço robusto para auxiliar a equilibrar os interesses da liberdade/segurança.

As capacidades de aplicação de IA, no âmbito da prevenção e repressão da criminalidade, conforme identificadas pelos vários autores e agregadas na Tabela n.º 1 (p. 4) do presente estudo, representam um contributo positivo inegável, mas com um custo para a liberdade e os valores éticos que a sociedade europeia não tem anuído a pagar. Resulta que, no ambiente da UE, a regulamentação mais atual, que integra o RGPD e o Regulamento de IA, pauta pela reafirmação do forte compromisso com a salvaguarda dos direitos fundamentais, de proteção de dados e da privacidade dos habitantes e transeuntes no seu território, não permitindo que os interesses genéricos da segurança se sobreponham à liberdade.

Por regra, ambos os normativos proíbem as práticas relacionadas com a recolha de dados biométricos ou aplicações de IA em espaços públicos, salvo em circunstâncias excecionais. Não obstante, os documentos são permeáveis quanto às obrigações gerais de recolha, tratamento e análise de dados pessoais, no sentido em que conferem possibilidade aos Estados-Membros para especificarem ou limitarem, através da transposição para a sua esfera de responsabilidade interna, os termos em que parte da regulamentação não se aplica, salientando-se os fins previstos para a garantia da segurança nacional, da defesa e da segurança pública.

Comparando com o panorama internacional, conclui-se que os EUA possuem uma abordagem de fragmentação legal quanto a esta matéria, procurando conjugar a sua visão de mercado liberal e orientada para a inovação tecnológica, com uma estratégia governamental proativa para lidar com os desafios e minimizar o impacto social dos sistemas de IA. Por sua vez, a falta de regulamentação robusta sobre direitos fundamentais e privacidade na China, evidencia um modelo onde a

segurança interna prevalece sobre as liberdades individuais, sendo a videovigilância com IA amplamente usada como instrumento central para o controlo social.

Reiterando a pergunta de partida, conclui-se que a implementação da videovigilância com IA na UE ocorre numa conjuntura de elevado escrutínio legal e ético, diferenciando-se do modelo flexível dos EUA e do autoritarismo digital da China. A UE opta pautar pelo equilíbrio, submetendo a inovação tecnológica ao respeito dos direitos fundamentais e não abdicando da reflexão sobre os seus verdadeiros impactos na vida dos cidadãos, perpetuando o desafio de assegurar que tais normativos não comprometam a eficácia dos sistemas de segurança e defesa, nem coloquem a UE em desvantagem competitiva face a outras potências tecnológicas.

REFERÊNCIAS BIBLIOGRÁFICAS

Abba, S., Bizi, A., Lee, J., Bakouri, S. e Crespo, M., 2024. Real-time object detection, tracking, and monitoring framework for security surveillance systems. *Heliyon*, Volume 10, Issue 15, 2024. https://www.sciencedirect.com/science/article/pii/S240584402410953X

Assembleia Parlamentar do Conselho da Europa [APCE], 2008. Video surveillance of public areas. Resolução n.º 1604, de 25 de janeiro de 2008. https://pace.coe.int/en/files/17633/html

Autoridade Europeia para a Proteção de Dados [AEPD], 2013. European Data Protection Supervisor Factsheet 4 – Keeping an eye on video-surveillance in the EU administration, 16 de dezembro de 2013. https://www.edps.europa.eu/data-protection/our-work/publications/factsheets/factsheet-4-keeping-eye-video-surveillance-eu_en

Berardini, D., Migliorelli, L., Galdelli, A. e Marín-Jiménez, M. J., 2025. Edge artificial intelligence and super-resolution for enhanced weapon detection in video surveillance. *Engineering Applications of Artificial Intelligence*, Vol. 140, 15 de janeiro de 2025. https://doi.org/10.1016/j.engappai.2024.109684

Comité Europeu para a Proteção de Dados [CEPD], 2010. The EDPS Video-Surveillance Guidelines, 17 de março de 2010. https://www.edps.europa.eu/sites/default/files/publication/10-03-17_video-surveillance_guidelines_en.pdf

Comité Europeu para a Proteção de Dados [CEPD], 2020. Guidelines 3/2019 on processing of personal data through video devices, Versão 2.0, adotada em

29 de janeiro de 2020. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_en_0.pdf

Finn, R. L., Wright, D., 2016. Privacy, data protection and ethics for civil drone practice: A survey of industry, regulators and civil society organisations. *Computer Law & Security Review*, 32, 2016, 577-586. http://dx.doi.org/10.1016/j.clsr.2016.05.010

Fontes, C., Hohma, E., Corrigan, C. C. e Lütge, C., 2022. AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society*, 71, 2022. https://doi.org/10.1016/j.techsoc.2022.102137

Frois, C., 2014. Book Review of Björklund and Svenonius "Video Surveillance and Social Control in a Comparative Perspective". *Surveillance, Gaming & Play*, Vol. 12, No. 3, 19 de junho de 2014, 466-467. https://doi.org/10.24908/ss.v12i3.5290

Irene, S., Prakash, A. J. e Uthariaraj, V. R., 2024. Person search over security video surveillance systems using deep learning methods: A review. *Image and Vision Computing*, 143, 2024. https://doi.org/10.1016/j.imavis.2024.104930

Lysova, T., 2025. Intersecting perspectives: Video surveillance in urban spaces through surveillance society and security state frameworks. *Cities*, Volume 156, 2025. https://doi.org/10.1016/j.cities.2024.105544

Miranda, W. D., Reis, J. F., Netto, R. M. e Santos, J. F., 2023. *Segurança Pública e Atividade de Inteligência: debates e perspetivas – Vol. II*. Belém – Pará: Érgane.

Murray, C., 2023. U. S. Data Privacy Protection Laws: A Comprehensive Guide. *Forbes*, 21 de abril de 2023. https://www.forbes.com/sites/conormurray/2023/04/21/us-data-privacy-protection-laws-a-comprehensive-guide

Parlamento Europeu e Conselho da União Europeia [PECUE], 1995. Diretiva n.º 95/46/CE, de 24 de outubro: Proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial das Comunidades Europeias, n.º L 281, 31-39. http://data.europa.eu/eli/dir/1995/46/oj

Parlamento Europeu e Conselho da União Europeia [PECUE], 2012. Tratado sobre o Funcionamento da União Europeia (Versão Consolidada). Jornal Oficial da União Europeia, n.º C 326, 1-390, 26 de outubro de 2012. https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF

Parlamento Europeu e Conselho da União Europeia [PECUE], 2016a. Regulamento n.º 679/2016, de 27 de abril: Regulamento Geral de Proteção de Dados. Jornal Oficial da União Europeia, n.º L 119, 1-88. http://data.europa.eu/eli/reg/2016/679/2016-05-04

Parlamento Europeu e Conselho da União Europeia [PECUE], 2016b. Carta dos Direitos Fundamentais da União Europeia. Jornal Oficial da União Europeia, n.º C 202, 389-405, 07 de junho de 2016. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT

Parlamento Europeu e Conselho da União Europeia [PECUE], 2024. Regulamento n.º 1689/2024, de 13 de junho: Regulamento da Inteligência Artificial. Jornal Oficial da União Europeia, Série L, 1-144. http://data.europa.eu/eli/reg/2024/1689/oj

Pfau, M., 2024. Artificial Intelligence: The New Eyes Of Surveillance. *Forbes*, 2 de fevereiro de 2024. https://www.forbes.com/councils/forbestechcouncil/2024/02/02/artificial-intelligence-the-new-eyes-of-surveillance

Piton, A., 2024. Inteligência Artificial e Reconhecimento Facial: Novas Fronteiras Penais?. *Ciências Criminais e Inteligência Artificial*, 77-89. Edições Almedina.

Ramos, A. D., 2023. A IA e a sua aplicação na Investigação Criminal: Contributo para a Identificação de Perfis na Criminalidade Organizada. *Anatomia do Crime*, n.º 17 (janeiro-junho 2023), 159-168.

Roser, M., 2022. Artificial intelligence is transforming our world – it is on all of us to make sure that it goes well. *Our World in Data*. https://ourworldindata.org/ai-impact

Sahin, K., 2020. The West, China, and AI surveillance. In *Atlantic Council*, GeoTech Cues, 18 de dezembro de 2020. https://www.atlanticcouncil.org/blogs/geotech-cues/the-west-china-and-ai-surveillance

Wang, S., Zhang, Y., Xiao, Y. e Liang, Z., 2025. Artificial intelligence policy frameworks in China, the European Union and the United States: An analysis based on structure topic model. *Technological Forecasting & Social Change*, 212, 2025 (aceite para publicação). https://doi.org/10.1016/j.techfore.2025.123971

Wright, D., Rodrigues, R., Raab, C., Jones, R., Székely, I., Ball, K., Bellanova, R. e Bergersen, S., 2015. Questioning surveillance. *Computer Law & Security Review*, 31, 2015, 280-292. http://dx.doi.org/10.1016/j.clsr.2015.01.006

ESTUDO 7 – O PAPEL DA INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO CRIMINAL

THE ROLE OF ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATION

Sara Isabel Rosado dos Santos Vale
Capitão GNR

RESUMO

O artigo em questão contempla uma análise relativa ao papel da inteligência artificial na investigação criminal, avaliando quais as suas potencialidades, limitações e desafios no contexto contemporâneo da segurança interna.

A análise evidencia como a inteligência artificial representa uma ferramenta transformadora para as atividades de prevenção criminal e investigação criminal, proporcionando capacidades avançadas de predição de zonas de risco, reconhecimento facial, identificação biométrica, análise forense e reconstrução de cenários criminais. Estas aplicações permitem uma alocação eficaz de recursos policiais e uma identificação célere de suspeitos.

Contudo, a implementação destes sistemas suscita questões éticas e jurídicas significativas, nomeadamente, quanto à salvaguarda dos direitos fundamentais dos cidadãos e à transparência algorítmica. A problemática da responsabilização nos processos de decisão automatizados e o fenómeno das "black boxes" constituem desafios adicionais.

O Regulamento Europeu da inteligência artificial emerge como um instrumento normativo fundamental, estabelecendo requisitos rigorosos para a utilização de sistemas classificados como de alto risco, embora a sua implementação represente um desafio complexo para os sistemas jurídicos nacionais.

Conclui-se que, apesar do seu potencial transformador, a utilização da inteligência artificial na investigação criminal deve ser acompanhada por um escrutínio rigoroso e de um enquadramento legal adequado que salvaguarde os valores democráticos.

Palavras-chave: Inteligência Artificial; Investigação Criminal; Regulamento Europeu da Inteligência Artificial; Direitos Fundamentais.

ABSTRACT

The article in question contains an analysis of the role of artificial intelligence in criminal investigation, evaluating its potential, limitations, and challenges in the contemporary context of internal security.

The analysis shows how artificial intelligence represents a transformative tool for criminal prevention and criminal investigation activities, providing advanced capabilities for predicting risk zones, facial recognition, biometric identification, forensic analysis, and reconstruction of crime scenes. These applications allow for effective allocation of police resources and swift identification of suspects.

However, the implementation of these systems raises significant ethical and legal questions, particularly regarding the safeguarding of citizens' fundamental rights and algorithmic transparency. The issue of accountability in automated decision-making processes and the phenomenon of "black boxes" constitute additional challenges.

The Artificial Intelligence Act emerges as a fundamental normative instrument, establishing rigorous requirements for the use of systems classified as high-risk, although its implementation represents a complex challenge for national legal systems.

It concludes that, despite its transformative potential, the use of artificial intelligence in criminal investigation must be accompanied by rigorous scrutiny and an appropriate legal framework that safeguards democratic values

Keywords: *Artificial Intelligence; Criminal Investigation; Artificial Intelligence Act; Fundamental Rights.*

1. INTRODUÇÃO

O impulso tecnológico contemporâneo tem desencadeado uma profunda metamorfose societal, caracterizada pelo advento de uma nova era digital, frequentemente conceptualizada como a "quarta revolução industrial". A Inteligência Artificial (IA) apresenta-se como um constructo tecnológico de amplitude transformadora, cujas múltiplas aplicações se estendem a um espectro alargado de domínios: desde processos de reconhecimento e catalogação de imagem, tradução automática de conteúdos textuais, elaboração de diagnósticos e prognósticos médicos com elevada precisão, até à pilotagem autónoma de dispositivos tecnológicos como drones e veículos, e inclusive à produção criativa de conteúdos artísticos, como composições musicais (Martins, 2022).

Na esteira dessas transformações na sociedade, hodiernamente, a criminalidade, particularmente nas suas vertentes mais graves, organizadas e transnacionais, caracteriza-se por desafios de crescente complexidade e amplitude, impulsionando as entidades competentes pela prevenção e investigação criminal a desenvolverem abordagens tecnologicamente avançadas que permitam uma resposta eficaz e atempada (Proença, 2023). Destarte, emerge a aplicação de

tecnologias como a IA às atividades de prevenção e Investigação Criminal (IC) desenvolvidas pelas polícias.

Segundo um inquérito realizado pela EUROPOL a cidadãos europeus, em fevereiro de 2022, constante no relatório *Accountability Principles for Artificial Intelligence in the Internal Security Domain*, 89,7% dos cidadãos concordaram que a IA fosse utilizada para a salvaguarda de crianças e grupos vulneráveis; 87,1% concordaram que a IA devia ser utilizada para identificar organizações criminosas e suspeitos; e 78,6% consideraram que a IA devia ser utilizada para prever crimes antes destes sucederem (Elias, 2024).

Este trabalho pretende assim responder à questão central "Quais as potencialidades, limitações e desafios da utilização da IA na Investigação Criminal?" e para tal utilizou-se uma metodologia qualitativa através de análise documental, incluindo estudos de casos realizados em diversos países. O trabalho encontra-se estruturado em quatro pontos onde no primeiro ponto será realizada uma nota introdutória, no segundo uma breve contextualização da IA, abrangendo a sua conceptualização, as suas aplicações e a legislação existente sobre o tema, no terceiro ponto serão apresentadas as potencialidades, limitações e os desafios associados à utilização da IA nas atividades de prevenção e IC e por fim serão apresentadas as conclusões e reflexões críticas que decorrem do presente estudo.

2. CONTEXTUALIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL

2.1. Concetualização

A pré-história da IA pode ser contemplada através de uma perspetiva arqueológica do conhecimento tecnológico, com a invenção da primeira máquina de calcular, por Wilhelm Schickard, em 1623, ou, num período temporal mais próximo da atualidade, com a invenção do primeiro modelo de computador com capacidade para armazenar e processar informação, em 1936, pelo britânico, frequentemente reconhecido como "pai da IA", Alan Turing (Rigano, 2019; Nunes *et. al*, 2024). No entanto, é em 1943 que surge o primeiro artigo científico de IA, no qual Warren McCulloch e Walter Pitts, propõem um modelo computacional para redes neurais (Martins, 2022; Russel, et al citado em Ramos, 2024).

Em 1956, Jonh McCarthy, cientista informático, define o termo "inteligência artificial" como a inteligência "de máquinas capazes de desempenhar tarefas características da inteligência humana" (Ramos, 2024) tendo como referência os conceitos desenvolvidos por Turin que salientaram que o desempenho

(comportamento de tipo inteligente) seria o foco da definição de inteligência (Kissinger, et al, 2021).

A produção do *Chatbot* Eliza, em 1965, deu origem à IA generativa, que assume tal designação por se tratar de um sistema automatizado que através de uma solicitação humana em linguagem comum, emprega algoritmos para produzir, manipular ou sintetizar dados, manifestando-se predominantemente em forma de textos e imagens. Este foi o primeiro software que permitiu reproduzir interações verbais, constituindo-se como um marco da evolução da IA a nível mundial (Nunes *et. al*, 2024; Ramos, 2024).

Observou-se, subsequentemente, uma progressão paradigmática consonante com os períodos históricos em questão, sendo que a evolução desta tecnologia cresceu a um ritmo desmesurável a partir de 2016 (Moleirinho *et. al*, 2024). Em 2017, foram desenvolvidos os domínios do reconhecimento da fala e da tradução, em 2021 surge o GPT (*Generative Pre-trained Transformer*) – 3 e em seguida o Chat GPT (Ramos, 2024).

Numa perspetiva holística, a IA pode ser considerada uma disciplina de estudo e de investigação que tem como principal escopo dotar os computadores de capacidades para efetuarem o tipo de tarefas e ações que os cérebros humanos executam (Boden citado em Martins, 2022). O grupo de trabalho sobre a IA do Parlamento Europeu considerou que a IA consiste na "capacidade que uma máquina tem para produzir competências semelhantes às humanas como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade" (Ramos, 2024).

Conforme estabelecido no Livro Branco sobre a IA, esta "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" (Comissão Europeia, 2020, p 2). Os dados, os algoritmos e o tratamento dos dados por uma máquina emergem, assim, estritamente correlacionados (Comissão Europeia citado em Magrani & Silva, 2022).

Adicionalmente, o recente Regulamento (UE) 2024/1689, do Parlamento Europeu e do Conselho, adiante designado de Regulamento Europeu da IA, refere que a IA é um conjunto de tecnologias com uma evolução galopante que conduz a variados benefícios em diversas áreas e que pode conferir vantagens competitivas

a diversos domínios dos Estados como a segurança e a justiça[81]. Não se focando tanto na sua definição mas sim no seu propósito, no que concerne aos sistemas de IA, o aludido Regulamento estatui que "o conceito de «sistema de IA» constante do presente regulamento deverá ser definido de forma inequívoca (…) concebendo a flexibilidade suficiente para se adaptar a rápidas evoluções tecnológicas neste domínio" acrescentado que "deverá basear-se nas principais características de IA que o distinguem de sistemas de *software* ou abordagens de programação tradicionais mais simples"[82].

O regulamento recentemente aprovado foca-se, fundamentalmente, na utilização dos sistemas de IA e nos riscos que dessa utilização possam advir definindo, assim, o sistema de IA como um "sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis (…) que com base nos dados de entrada que recebe, infere a forma de gerar resultados (…) que podem influenciar ambientes físicos ou virtuais"[83].

Relativamente à tipologia, a IA pode ser referente a *softwares*, como são os casos dos assistentes virtuais, dos softwares de análise de imagem, dos motores de busca e dos sistemas de reconhecimento facial e de voz ou integrada em *hardware*, como se constata no caso dos robôs, dos carros autónomos, dos drones ou das aplicações no âmbito da internet das coisas (Parlamento Europeu, 2020).

2.2. Aplicações da Inteligência Artificial

A IA tem vindo a ganhar uma presença cada vez mais significativa no quotidiano de todos os cidadãos (Rigano, 2019), fundamentalmente, devido a dois fatores cruciais: a disponibilidade de uma vasta quantidade de bases de dados e a necessidade premente de processar a informação que delas decorre, de forma eficiente (Ramos, 2023).

Esta tecnologia consegue analisar notáveis quantidades de dados e fornecer perspetivas que podem auxiliar a tomar decisões numa variedade de negócios. No geral, a importância da IA reside na sua capacidade de automatizar, personalizar, melhorar o processo de tomada de decisões, aumentar a eficiência e impulsionar

---

81 Ponto (4) do preâmbulo do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho.
82 Ponto (12) do preâmbulo do Regulamento (EU) 2024/1689 do Parlamento Europeu e do Conselho.
83 Número 1) do art.º 3.º do Regulamento (EU) 2024/1689 do Parlamento Europeu e do Conselho.

a inovação, tornando-a numa tecnologia crucial tanto para empresas como para indivíduos (Gund *et. al*, 2023).

Hodiernamente, a IA é aplicada em diversos domínios, podendo sempre ser incompleta a lista apresentada (Martins, 2022), assim serão apenas referenciados alguns exemplos.

No domínio da justiça, a IA pode ser utilizada para pesquisar jurisprudência, ou, por exemplo para adotar medidas de justiça tendo como base casos passados idênticos aos que se encontram em análise; no domínio da saúde, a identificação do diagnóstico e da intervenção terapêutica necessária podem evoluir significativamente com o auxílio da IA; na área da ciência, a tecnologia pode ser utilizada no aperfeiçoamento do desenho, na descoberta de novas moléculas e na análise e correlação de dados; no domínio das finanças, a IA pode ser usada nos mercados financeiros para a avaliação do risco ou para a identificação de fraudes; ao nível da segurança informática, a tecnologia contribui fortemente para a cibersegurança; e no domínio da defesa e segurança nacional pode ser utilizada, por exemplo, na marcação de alvos por satélites (Nunes *et. al*, 2024).

Não sendo uma exceção, tal como em todas as áreas do conhecimento, as aplicações da IA começam também a ganhar palco em diversas aplicações de utilização por parte das Forças e Serviços de Segurança (Moleirinho *et. al*, 2024) e sob esse aspeto, mais especificamente também no domínio da IC.

2.3. Enquadramento normativo da Inteligência Artificial

O advento IA tem suscitado profundas transformações na sociedade contemporânea, configurando-se como um dos maiores desafios regulatórios do século XXI. A necessidade premente de estabelecer um quadro normativo para a IA estabelece a sua evidência desde o ano de 2018, tendo sido criados para o efeito grupos de trabalho em diversos Estados, sendo ainda de realçar as contribuições de entidades não governamentais (Martins, 2022).

Ao nível internacional, destacam-se, primordialmente, dois instrumentos normativos, a Recomendação da UNESCO sobre a Ética da IA, onde são apresentados quatro valores e dez princípios fundamentais que lhes estão subjacentes e o Guia da Organização Mundial de Saúde sobre Ética e Governação da IA para a Saúde (Nunes *et. al*, 2024).

O esforço pioneiro de estabelecer um enquadramento legislativo transversal para a IA é atribuído incontestavelmente à UE (Martins, 2022). Em 2018, foi aprovada a "Carta Europeia de Ética sobre o Uso da Inteligência Artificial em Sistemas Judiciais e respetivo Ambiente" e em 2021, surgiu a Proposta de Regulamento do Parlamento Europeu e do Conselho, que estabelece regras harmonizadas em matéria de IA e que alterou determinados atos administrativos. Recentemente, em março de 2024, foi aprovado o Regulamento do Parlamento Europeu e do Conselho que Estabelece Regras Harmonizadas em Matéria de IA (Valente, 2024), sendo o mesmo aplicável a partir do dia dois de agosto de 2026, com a exceção de alguns capítulos que terão aplicabilidade desde o dia dois de fevereiro de 2025.

O Regulamento Europeu da IA contempla um quadro regulamentar que define quatro níveis de risco para os sistemas de IA, designadamente, o risco mínimo, o risco limitado, o risco elevado e o risco inaceitável (Sousa, 2024).

No âmbito do presente estudo importa referir que são considerados sistemas de risco inaceitáveis os que se destinam à avaliação ou classificação de pessoas singulares ou grupos de pessoas, durante um certo período, com base no seu comportamento social ou em caraterísticas de personalidade ou pessoais conhecidas, inferidas ou previsíveis em que a classificação social leve a um tratamento desfavorável a essas pessoas, e os que efetuam avaliações de risco das pessoas cometerem uma infração penal, com base exclusivamente na definição de perfis ou na avaliação dos seus traços e características de personalidade[84].

Além destes, acresce ainda a utilização de sistemas de identificação biométrica à distância, em tempo real, em espaços acessíveis ao público, com a exceção dos casos em que se procura uma vítima de um crime, para prevenção de ataques terroristas, em situações de ameaças à vida ou à integridade física e para procura de suspeitos ou arguidos[85].

A nível nacional ainda não se encontra aprovado qualquer instrumento legal específico relativamente à utilização de sistemas de IA, embora a modernização da Administração Pública seja um dos elementos fundamentais estabelecidos para a transição digital pelo governo português, onde a IA se inclui como um dos principais vetores (Neves, 2024).

---

[84] Conforme alíneas c) e d) do artigo 5.º do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho.

[85] Conforme artigo 5.º do Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho.

3. INTELIGÊNCIA ARTIFICIAL NA INVESTIGAÇÃO CRIMINAL: POTENCIALIDADES, LIMITAÇÕES E DESAFIOS

A segurança interna, tal como definido no número (n.º) 1, do artigo 1.º da Lei de Segurança Interna, pode ser definida como "a atividade 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"[86].

A prevenção e repressão da criminalidade é assim uma das finalidades fundamentais da segurança interna. Para concretização de tal desiderato concorrem duas atividades, designadamente, a prevenção criminal e a IC que, embora estejam fortemente interligadas, são atividades distintas.

A prevenção criminal constitui uma das atribuições nucleares da polícia e opera em três dimensões distintas: a primeira onde são consideradas as componentes de natureza urbanística, o design do meio ambiente, o policiamento de proximidade efetuado pelas polícias e a educação e prevenção geral; a segunda em que as componentes consideradas são as relacionadas com as zonas de alta incidência criminal, a identificação dos delinquentes e envolvimentos com grupos organizados e a referenciação dos principais tipos de crime ou criminalidade; e a terceira que engloba a IC, os meios de obtenção de prova, a detenção, a acusação e a condenação (Noronha, 2022). Conforme refere Moleirinho *et. al* (2024, p. 216), "ao policiamento preventivo cumpre antecipar os riscos de comportamentos desviantes, no limite, com contornos criminais".

A IC "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", conforme previsto no artigo 1.º da Lei de Organização da Investigação Criminal, aprovada pela Lei n. º49/2008, de 27 de agosto.

No que respeita à atividade de prevenção criminal, a IA tem vindo a ser explorada aquando da aplicação de modelos de policiamento mais preventivos,

[86] Aprovada pela Lei n.º 53/2008, de 29 de agosto.

mormente, pelas capacidades de análise de um grande volume de dados que proporciona (Moleirinho et. al, 2024). A par de outras tecnologias, como afirma Ratcliffe (citado em Moleirinho et. al, 2024), a IA tem sido uma ferramenta auxiliar no que concerne à análise de ADN, à análise das redes sociais e das comunicações telefónicas, às movimentações eletrónicas de capitais e à videovigilância com reconhecimento facial. Podem ainda ser acrescentadas as aplicações da IA em "identificação de perfis suspeitos; o controlo de tráfego; a análise de movimentos bancários na dark web; a deteção de pornografia infantil e a deteção de padrões anormais na vigilância de espaços públicos" (Raaijmakers citado em Moleirinho et. al, 2024, p. 204).

Esta tecnologia tem assim potencialidades consideráveis para prevenir a criminalidade e servir de método auxiliar no direcionamento dos recursos para determinados locais, nos momentos em que estes se lá tornem prementes (Santos, 2023).

As aplicações da IA às funções policiais, e mais concretamente à prevenção criminal e IC, não são estanques, ou seja, a utilização do mesmo sistema de IA pode ser utilizado, quer nas atividades de prevenção criminal, quer nas atividades de IC. Como exemplos particulares da aplicação da IA às funções policiais de prevenção criminal ou IC podem enumerar-se os seguintes: reconhecimento de imagem, com deteção da expressão facial; a identificação de emoções; o reconhecimento de voz e de comportamentos suspeitos relativos a alterações da ordem pública; a pesquisa de pessoas desaparecidas; a monitorização das redes sociais; a utilização de 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 (Moleirinho et. al, 2014).

Enquanto ferramenta de predição de atividades criminais, a IA pode ser direcionada para identificar os locais de risco (*hot spot policing*), através da análise de dados históricos constantes nas bases de dados das polícias, permitindo uma alocação eficaz dos seus recursos, ou para o risco dos indivíduos (*heat lists*). As *heat lists* consistem em listas que identificam pessoas propensas a cometer crimes (Santos, 2023; Ramos 2024).

Os *hot spot policing* têm sido uma prática bastante criticada pelos erros que deles têm decorrido, podendo os mesmos resultar, essencialmente, dos dados inseridos para análise estarem viciados e do algoritmo se constituir ou criar um ciclo discriminatório. Santos (2023), refere, como exemplo, o sucedido nos EUA,

ao nível do Direito de Mera Ordenação Social, em que a concentração geográfica das fiscalizações e as inspeções centradas em empresas com determinadas características levou a que se verificasse um crescente número de casos detetados e, consequentemente, à alocação de recursos para ações de fiscalização na zona geográfica em questão, deixando outras áreas sem qualquer fiscalização.

Os sistemas de informação geográfica, por sua vez, são instrumentos de mapeamento digital do crime que funcionam em tempo real, através de algoritmos de constatação de padrões. Estes sistemas não se constituem por si só num instrumento de IA, mas ao poder aliar tal tecnologia, torna-se possível obter uma reconhecível capacidade analítica das bases de dados, que se configuram cada vez mais complexas, conseguindo uma capacitação exponencial dos modelos de policiamento preditivos (McDaniel & Pease citado em Moleirinho et. al, 2024).

Ainda no âmbito da predição, importa abordar a utilização de tecnologia biométrica e particularmente, a de reconhecimento facial, que aliada aos programas de desenvolvimento de IA, se constitui uma realidade presente em 80% da população mundial, nos quatro cantos do mundo (Piton, 2024). Esta tecnologia permite identificar possíveis autores de um crime com base na análise dos dados corporais, como a forma de andar, a postura e a face, bem como, para analisar expressões faciais, inflexões, pausas e hesitações numa inquirição de testemunha, e padrões na escrita, para reconhecimentos emocionais e de estados psicológicos (Santos, 2023).

O uso da tecnologia biométrica aliado à IA, demonstra a sua utilidade prática na predição de futuros eventos terroristas, estando neste campo, a aplicabilidade da IA consideravelmente desenvolvida. Neste âmbito, a referida tecnologia é fundamental pois permite simplificar a constatação de fenómenos terroristas orquestrados na internet e localizar os rostos dos potenciais suspeitos, bem como as suas passagens por locais públicos com vigilância, através de uma análise de milhares de dados disponibilizados, num período temporal ínfimo (Ramos, 2023).

O próprio Regulamento Europeu da IA, no seu artigo 3.º, diferencia os sistemas de identificação biométrica à distância dos sistemas biométricos à distância em tempo real. O sistema de identificação biométrica à distância para fins policiais, em espaços públicos, consagrado no referido regulamento, embora seja classificado como de risco elevado, é autorizado, excecionalmente, nos casos da procura de vítimas específicas de crimes, incluindo crianças desaparecidas, de resposta a uma ameaça iminente de ataque terrorista ou na localização e identificação dos autores de crimes graves (Piton, 2024).

No que concerne particularmente ao reconhecimento facial, este pode assumir a modalidade estática, quando se comparam imagens captadas com as que constam em bases de dados, ou dinâmica, em que a análise das imagens é realizada em tempo real, procurando-se uma comparação imediata com os dados que se encontram em arquivo, relativos à pessoa que se pretende identificar (Smith *et. al*. citado em Smith & Miller, 2022).

A utilização dos sistemas de reconhecimento facial pode ser diferenciada quanto à sua finalidade, nomeadamente para efeitos preventivos ou para efeitos de IC. Para efeitos de IC, a tecnologia demonstra ser fundamental para estabelecer a identidade ou a localização de um indivíduo suspeito, ultrapassando as limitações decorrentes do facto da análise da extensa quantidade de registos imagéticos e videográficos potencialmente pertinentes, constituir, para a componente humana, uma tarefa morosa e meticulosa suscetível a imprecisões, decorrentes, entre outros fatores, da fadiga. Os sistemas computacionais apresentam como vantagem a capacidade de processamento ininterrupta (Rigano, 2019).

Para efeitos preventivos, se não houver uma regulamentação precisa, o procedimento pode significar uma afronta à liberdade e privacidade individuais (Raposo, 2023). Acresce que a sua utilização nesta vertente se tem mostrado pouco eficaz, dando-se o exemplo da cidade de Londres, conhecida mundialmente pela utilização das câmaras de vigilância, que nas duas décadas passadas sofreu 13 ataques terroristas, sendo metade deles no mesmo ano, em 2017 (Piton, 2024).

No que concerne à atividade de IC, a IA pode ser utilizada ao nível da recolha da prova, assumindo uma de quatro formas, como instrumento de recolha de prova, constituir ela própria prova, produzir ela própria prova e ser meio de valoração de prova (Santos, 2023).

Neste âmbito, e podendo constituir elemento de recolha de prova, produzir ela própria prova ou ser meio de valoração de prova, a IA pode ser utilizada para analisar evidências digitais através do estudo de elevadas quantidades de provas que se encontram no universo digital, como por exemplo, registos de chamadas ou atividades em redes sociais, e-mails e mensagens para ajudar a reconstruir eventos e detetar eventuais suspeitos (Ramos, 2024).

Como exemplo concreto do explanado, foi desenvolvido um caso real de análise de anúncios de tráfico de armas na *dark web*, através da aplicação de mecanismos de IA. O objetivo foi através de dados utilizados nesses anúncios, tais como, nome do mercado, nome do vendedor, país de onde o item seria

enviado, hora em que o anúncio foi publicado e outros, poder constatar padrões e relações. O sistema, através da análise dos dados, estabeleceu correspondências que mostraram a sua aplicabilidade prática, tendo sido validado pelas autoridades policiais (Fernandez-Basso et. al, 2024).

No que concerne à cibercriminalidade, tem-se verificado a crescente implementação de ferramentas alicerçadas em IA, designadamente, para fazer face a ataques virais, burlas por via de *phishing*, operações financeiras fraudulentas e usurpação de identidade. Neste domínio, a IC apresenta progressos significativos na identificação de padrões comportamentais dos utilizadores, deteção de anomalias ou discrepâncias e sinalização de transações de carácter duvidoso. As agências que utilizam estes sistemas manifestam capacidade acrescida na deteção e prevenção de ilícitos, bem como na identificação e neutralização de ataques de software malicioso, nomeadamente, ransomware, potencialmente lesivo para infraestruturas informáticas (Faqir, 2023).

Com o mesmo propósito pode a IA ser aplicada na análise forense avançada através dos vestígios encontrados no local do crime, como impressões digitais, machas de sangue, entre outros, identificando detalhes que seriam impercetíveis para um ser humano (Ramos, 2024).

Relativamente à análise e comparação de impressões digitais, por exemplo, a IA pode vir a prestar um auxílio revolucionário. Através de um estudo publicado na revista intitulada "Associação Americana para o Avanço da Ciência", em janeiro de 2024, implementado com recurso a IA, foi possível comprovar, com 99,99% de certeza, que as impressões digitais intrapessoais detêm convergências muito significativas, sendo que tais convergências são válidas para todos os pares de dedos da mesma pessoa, ainda que de mãos diferentes. Isto significa que ao invés da análise realizada até então, em que só era possível realizar a comparação de impressões do mesmo dedo exato, a dactiloscopia passa a ter capacidade para comparar impressões digitais que não correspondam de forma exata à registada, ganhando uma nova potencialidade enquanto meio de prova (Lourenço, 2024).

No que concerne à recriação do local do crime, a identificação de padrões característicos na análise balística apresenta-se como outra área propícia à aplicação de algoritmos de IA. A análise de registos sonoros de disparos captados por dispositivos móveis e aparelhos inteligentes pode contribuir significativamente para a investigação em curso, fundamentando-se tal importância na observação de que o conteúdo e a qualidade das gravações de disparos são condicionados pela

tipologia da arma de fogo e munição empregues, pela configuração espacial do cenário e pelo dispositivo de captação utilizado (Rigano, 2019).

Em face deste pressuposto, no âmbito de projetos europeus, em Portugal tem sido possível investir em sistemas de IA com diversas finalidades. Como exemplo, reportando-se ao programa Horizonte 2020, o Projeto Darlene desenvolveu uns óculos de realidade aumentada que, em articulação com outros recursos tecnológicos, possibilitam a reconstituição fidedigna do cenário criminal, proporcionando uma análise pormenorizada que transcende as limitações inerentes à observação presencial do local do crime (PJ, 2024).

Na área da medicina, os algoritmos de IA têm vindo a ser implementados na interpretação de exames imagiológicos, o que comporta relevantes implicações para a medicina legal e para a comunidade de especialistas em patologia forense no estabelecimento da causa e circunstâncias do óbito (Faqir, 2023).

A IA pode ainda constituir fonte de prova, ao integrar mecanismos que registam dados como a geolocalização, os batimentos cardíacos, a temperatura corporal, a pressão sanguínea e outros dados recolhidos através de sensores biológicos, por exemplo, incorporados em relógios inteligentes. Em 2019, nos EUA, a Alexa (o assistente pessoal desenvolvido pela Amazon) constituiu fonte de prova num caso de homicídio, através dos seus registos áudio que serviram como prova testemunhal. Ao nível europeu, em 2021, num caso ocorrido na Baviera, ocorreu situação semelhante (Santos, 2023).

A utilização de sistemas de IA, aliada a outros sistemas tecnológicos demonstra assim trazer inúmeras vantagens às atividades de prevenção criminal e IC, contudo, tem vindo a levantar questões de ordem ética, deontológica e de valoração dos direitos fundamentais das pessoas e da privacidade, constitucionalmente consagrados (Hunkenshroer & Luetge citado em Elias, 2024). O direito à privacidade, previsto no artigo 26.º do texto constitucional, bem como na Declaração Universal dos Direitos Humanos (artigo 12.º) e na Convenção Europeia dos Direitos Humanos (artigo 8.º) pode ficar assim comprometido (Moleirinho, 2024). Como afirma Hassemer (citado em Moleirinho, 2024) quando um Estado adota uma política focada no combate ao crime, com implicações na garantia da liberdade e salvaguarda dos direitos fundamentais dos cidadãos, pode colocar em causa os princípios do Estado de Direito Democrático.

Estas questões colocam-se mormente nos sistemas de prevenção criminal, que embora concorram para uma atividade essencial, não devem colocar em causa

a liberdade, a autonomia e a privacidade dos cidadãos. Como afirma Fontes (2022), "o chamado policiamento inteligente está carregado de vantagens, mas os riscos são graves e ainda não é possível recensear todo o seu universo", levantando assim o dilema prévio relativo ao equilíbrio entre a liberdade e a segurança.

No âmbito do Estado de Direito, a implementação de medidas de investigação tecnológicas, como é o caso da IA, deve observar um conjunto estruturante de princípios jurídicos basilares. O princípio da legalidade exige fundamentação legal prévia das medidas de investigação tecnológicas para restrições de direitos fundamentais, enquanto o princípio da jurisdicionalidade atribui, regra geral, ao juiz a competência exclusiva para autorização de diligências de recolha de prova. O princípio da especialidade impõe que as medidas investigativas estejam estritamente vinculadas a um processo criminal em curso, sendo vedada a sua utilização para fins preventivos ou prospetivos. Complementarmente, o princípio da idoneidade delimita o escopo subjetivo e objetivo das diligências, bem como a sua duração, em função da utilidade processual. Por fim, o princípio da proporcionalidade, nas suas vertentes de necessidade, adequação e proporcionalidade em sentido estrito, determina que a intensidade lesiva dos direitos fundamentais causada pelos sistemas tecnológicos em uso deve estar em consonância com a gravidade do ilícito, a sua relevância social e os objetivos processuais visados (Santos, 2023).

Aduz-se que, não sendo as polícias em princípio dotadas do conhecimento técnico especializado necessário para desenvolver os sistemas de IA, acabam por ser compelidas a externalizar esta competência técnica recorrendo a empresas privadas. Consequentemente, quando utilizado o sistema de IA para praticar qualquer ação, suscitam-se questões pertinentes quanto à natureza híbrida das decisões tomadas com base no sistema e ao enquadramento jurídico mais adequado para a sua regulação, uma vez que poder-se-á argumentar que a decisão resulta, pelo menos parcialmente, dos sistemas informáticos desenvolvidos por entidades privadas (Lanceiro, 2024).

Embora a necessidade de meios tecnológicos de recolha de dados desenvolvidos seja elencada como uma limitação, mormente, devido aos sistemas de IA se alimentarem dos dados que forem recolhidos e arquivados nas bases de dados, ao nível do reconhecimento facial, por exemplo, já se encontram a ser testados sistemas que se dedicam à reconstrução facial a partir de registos de baixa qualidade, incluindo imagens de reduzida resolução e iluminação ambiente

insuficiente, contextos nos quais a degradação do registo dificulta significativamente a correspondência facial (Rigano, 2019).

Adicionalmente, esta tecnologia poderá resultar nas chamadas "black boxes", que significa que os mecanismos internos que conduziram a determinado resultado, transcendem frequentemente a capacidade de compreensão humana, mormente para indivíduos destituídos de formação tecnológica especializada. A ausência de transparência nos sistemas de IA configura um desafio multidimensional, contemplando desde estratégias deliberadamente opacas associadas a segredos comerciais até limitações decorrentes de analfabetismo tecnológico e características intrínsecas ao design computacional. Tal obscuridade não só compromete a salvaguarda de direitos fundamentais e princípios éticos, mas também cria obstáculos à identificação e correção de potenciais enviesamentos, discriminações algorítmicas silenciosas e manipulações comportamentais subtis (Magrani & Silva, 2022).

Como referido no caso dos *hot spot policing*, a aplicação de sistemas de IA pode ainda levar a resultados preconceituosos e discriminatórios. Os algoritmos, que operam, fundamentalmente, com base nos dados disponibilizados, podem produzir resultados problemáticos quando estes dados apresentam, *ab initio*, elementos discriminatórios intrínsecos. Questões críticas emergem quando os sistemas não são alimentados com dados adequadamente representativos, conduzindo, a título exemplificativo, a situações em que os sistemas de IA demonstram falhas sistemáticas no reconhecimento de grupos minoritários sub-representados em tecnologias como o reconhecimento facial. A experiência norte-americana é particularmente elucidativa neste aspeto: a utilização por parte das polícias de sistemas de reconhecimento facial baseados em IA revelou uma tendência discriminatória, afetando desproporcionalmente minorias raciais comparativamente à população caucasiana, bem como comunidades economicamente desfavorecidas em relação às mais abastadas (Lanceiro, 2024).

Surge ainda a questão da responsabilidade no contexto da utilização de sistemas de IA (Novais, 2023). Verifica-se, primeiramente, uma significativa incerteza quanto à determinação do sujeito responsável por um sistema de IA defeituoso, se a mesma deve ser assumida pelos serviços que compraram o sistema, se pela empresa que o desenvolveu ou se por ambos em corresponsabilidade. No que concerne especificamente a decisões erróneas resultantes da utilização de IA, observa-se que os titulares dos órgãos públicos podem, potencialmente,

invocar a natureza automatizada do processo decisório como fundamento para se eximirem de responsabilidade. Esta situação conduz a uma efetiva inoperância dos mecanismos de salvaguarda tradicionalmente estabelecidos, sejam eles no âmbito da responsabilidade disciplinar ou da responsabilidade civil. Importa salientar que um algoritmo ou código informático, per se, não pode ser constituído como sujeito de responsabilidade jurídica. Consequentemente, o que subsiste destes mecanismos de garantia é, fundamentalmente, a responsabilidade imputável ao próprio órgão público (Lanceiro, 2024).

Importa agora salientar que, tal como a utilização da IA se constitui como fator essencial para as polícias que desenvolvem as atividades de IC conseguirem alcançar atuações mais efetivas e eficazes (Proença, 2023), constitui também um desafio ao potencializar uma mudança exponencial nos padrões de crime com que as polícias se irão deparar.

No relatório *Tech Watch Flash* da EUROPOL, publicado em 2023, intitulado "Chat GPT – o impacto de modelos de linguagem grandes na aplicação da lei", foram identificadas algumas áreas de preocupação pelos peritos, nomeadamente as burlas e engenharia social: através da redação de textos realísticos, e por isso bastante credíveis, o ChatGPT constitui-se numa ferramenta de manipulação psicossocial, permitindo a simulação artificiosa de identidades (individuais ou de grupos específicos) suscetíveis de induzir comportamentos vulneráveis em potenciais vítimas de atividades criminosas; a desinformação e propaganda: uma vez que o programa proporciona aos seus utilizadores a capacidade de criar e difundir uma mensagem com um objetivo específico, através da conceção de conteúdos textuais com som fidedigno; e o cibercrime: ao habilitar criminosos com poucos conhecimentos técnicos a produzir códigos maliciosos, pela funcionalidade que a tecnologia detêm de gerar códigos em linguagens de programação distintas (Elias, 2024).

Na lista das tecnologias emergentes que se percecionaram como um desafio maior para a cibersegurança em Portugal, no ano de 2023, a IA ocupou a terceira posição, com 61% das respostas, conforme pode ser consultado no Relatório de Cibersegurança em Portugal, divulgado em julho de 2024. Relativamente ao ano de 2024, perspetiva-se que a IA, venha a ocupar a primeira posição na perceção sobre as tecnologias emergentes que representaram um maior desafio para a cibersegurança, com 94% das respostas. O aumento da desinformação com base em conteúdos de IA generativa surge, ainda, como uma tendência emergente com

impacto nacional que poderá marcar o futuro próximo do ciberespaço.

Poderemos ainda elencar como desafio futuro, a aplicabilidade do Regulamento Europeu de IA em Portugal ao nível da implementação normativa, designadamente na adaptação dos sistemas jurídicos e tecnológicos às exigências de transparência, segurança e ética algorítmica.

Até a entrada em vigor do Regulamento Europeu de IA, o Regulamento Geral de Proteção de Dados (RGPD) era aplicável, regra geral aos sistemas de IA, o que deixará de se tornar uma realidade, mormente porque o RGPD circunscreve-se ao processamento de dados pessoais, não abrangendo as decisões fundamentadas em grandes volumes de dados, como acontece com os sistemas de IA (Lanceiro, 2024).

O Regulamento Europeu de IA estabelece um quadro normativo particularmente exigente no que concerne aos sistemas de IA classificados como de alto risco, instituindo um conjunto significativo de deveres vinculativos, principalmente direcionados aos fornecedores destes sistemas. Entre as principais imposições normativas, destaca-se a implementação de um sistema robusto de gestão de riscos, a elaboração e manutenção de documentação técnica pormenorizada, e a garantia de registos automáticos de eventos durante todo o ciclo de vida do sistema. Adicionalmente, o regulamento estabelece requisitos rigorosos quanto à transparência operacional, exigindo que o funcionamento dos sistemas seja interpretável pelos responsáveis pela sua implementação. De particular relevância é a obrigatoriedade de supervisão humana efetiva, materializada através de interfaces adequadas, bem como a necessidade de assegurar níveis apropriados de exatidão, robustez e cibersegurança (Lanceiro, 2024).

A complexidade técnica do regulamento requer uma transformação profunda, implicando a necessidade de desenvolver mecanismos de avaliação de riscos, certificação de sistemas de IA e definição de protocolos rigorosos de monitorização, que garantam o cumprimento do preceituado no Regulamento, mas ao mesmo tempo terá potencialidade para evitar muitas das limitações ou preocupações expressas anteriormente.

A este propósito, numa perspetiva societal, a literacia digital e a compreensão dos sistemas de IA constituem imperativos contemporâneos, abrangendo desde o cidadão comum até aos dirigentes das empresas tecnológicas. O Plano de Ação para a Educação Digital (a ser aplicado entre 2021-2027) da Comissão Europeia exemplifica esta prioridade, tendo como objetivos estabelecidos melhorar as competências digitais dos cidadãos desde a infância, o que inclui investir em

conhecimentos basilares de IA, valores éticos subjacentes a essas tecnologias e consciencialização sobre a existência de direitos digitais. Tais medidas funcionariam como uma estratégia relevante para a redução de assimetrias informacionais, prevenindo riscos por meio do aumento da conscientização pública, da capacitação dos utilizadores e do consequente exercício efetivo dos seus direitos (Magrani & Silva, 2022).

Particular ênfase recai sobre a formação dos profissionais privados envolvidos nos processos de desenvolvimento destas tecnologias, exigindo-se não apenas proficiência técnica, mas também sólida compreensão das diretrizes éticas e jurídicas fundamentadas em valores democráticos e direitos humanos. Neste contexto, destaca-se outra iniciativa da Comissão Europeia de integrar princípios éticos no currículo de formação dos especialistas no desenvolvimento de sistemas de IA, estabelecendo um paradigma educacional holístico que conjuga competência técnica e responsabilidade social (Magrani & Silva, 2022).

4. CONCLUSÕES E REFLEXÕES CRÍTICAS

A presente investigação teve como objetivo analisar as potencialidades, limitações e desafios da utilização da IA na IC, tendo permitido alcançar conclusões significativas que evidenciam a complexidade e relevância desta tecnologia no contexto da justiça criminal.

A crescente utilização da IA na sociedade, a que assistimos nos últimos anos, está intrinsecamente relacionada com a explosão da quantidade de dados produzidos diariamente, fenómeno impulsionado pela digitalização acelerada e pela interconectividade global.

A complexidade inerente ao objeto de investigação em apreço manifesta-se, desde logo, na conceptualização e delimitação epistemológica da IA, revelando-se imperativo proceder a uma diferenciação rigorosa entre a mesma e os demais sistemas tecnológicos contemporâneos. Esta distinção fundamenta-se, primordialmente, na singular capacidade da IA para realizar processos inferenciais sofisticados.

A utilização desta tecnologia tem vindo a revolucionar sectores cruciais da sociedade, desde o campo da medicina até ao domínio educacional, não sendo por isso a sua aplicação nas funções policiais uma exceção. No que concerne especificamente à utilização dos sistemas de IA nas atividades de IC, esta tem vindo a revelar-se um vetor de transformação paradigmática, oferecendo avanços

significativos na eficiência e precisão dos processos de prevenção e repressão da criminalidade.

A IA manifesta inúmeras potencialidades de significativa relevância operacional, evidenciando-se como uma ferramenta transformadora no âmbito da prevenção e IC. A sua aplicabilidade estende-se desde a identificação preditiva de zonas de risco, possibilitando uma alocação otimizada de recursos policiais, até à implementação de sistemas biométricos e, particularmente, de reconhecimento facial, que no combate ao terrorismo, permitem a identificação e localização célere de suspeitos. No domínio do combate à cibercriminalidade, a tecnologia demonstra-se crucial na deteção de padrões comportamentais suspeitos e anomalias em transações digitais conferindo acrescida capacidade na prevenção e deteção de ilícitos. A análise forense avançada beneficia igualmente desta tecnologia, que permite a identificação de pormenores impercetíveis aos olhos humanos, em vestígios forenses. Complementarmente, na reconstituição digital do local do crime, possibilita uma análise meticulosa e fidedigna do cenário criminal, transcendendo as limitações da observação presencial e proporcionando uma compreensão mais profunda dos eventos ocorridos.

Contudo, a utilização destas tecnologias não está isenta de desafios e limitações que impõem uma reflexão crítica sobre o seu impacto e implicações éticas e jurídicas. Alguns dos debates suscitados neste contexto não são exclusivos do advento da IA, mas remontam a questões de longa data.

A implementação de sistemas de IA no contexto da prevenção e IC suscita profundas questões de ordem ética, deontológica e axiológica, particularmente, no que concerne à salvaguarda dos direitos fundamentais constitucionalmente consagrados. Esta tecnologia, não obstante as suas potencialidades transformadoras, confronta-nos com o dilema ancestral entre liberdade e segurança, exigindo uma ponderação criteriosa entre a eficácia operacional e a preservação das garantias individuais fundamentais.

No contexto do Estado de Direito Democrático, a aplicação de sistemas tecnológicos na IC deve respeitar um conjunto estruturante de princípios jurídicos fundamentais, garantindo a legalidade, a supervisão judicial, a especificidade das medidas, a adequação dos procedimentos e a proporcionalidade das intervenções. O cumprimento rigoroso destes princípios é essencial para assegurar que a utilização da IA se processa em conformidade com os valores democráticos e o devido processo legal. A este propósito surgem ainda as questões em matéria de

responsabilização uma vez que a natureza híbrida das decisões automatizadas pode diluir a atribuição de responsabilidade entre entidades públicas e privadas. Paralelamente, a opacidade dos algoritmos, conhecida como o problema das *black boxes*, compromete a transparência e a auditabilidade dos processos, dificultando a identificação de vieses, erros e potenciais discriminações algorítmicas.

O Regulamento Europeu da IA detém potencial para mitigar algumas das limitações atualmente associadas à utilização da IA, nomeadamente ao impor requisitos rigorosos de transparência, supervisão humana e mitigação de vieses algorítmicos. No entanto, a sua implementação representará um desafio significativo, exigindo a adaptação dos sistemas jurídicos e tecnológicos e a criação de mecanismos eficazes de monitorização e certificação.

Por fim, a evolução da criminalidade tecnológica impulsionada pela própria IA constitui um desafio crescente, exigindo das forças de segurança uma resposta ágil e inovadora. A cibercriminalidade, a disseminação de desinformação e a utilização da IA para fins ilícitos demonstram que esta tecnologia não é apenas um instrumento de combate ao crime, mas também um fator que reconfigura o próprio panorama criminal.

Em suma, a IA na IC apresenta um potencial significativo para melhorar a eficácia das forças de segurança, mas a sua implementação deve ser acompanhada de um escrutínio rigoroso, de um enquadramento legal adequado e de um compromisso inabalável com os princípios éticos e jurídicos que sustentam uma sociedade democrática.

REFERÊNCIAS BIBLIOGRÁFICAS

Centro Nacional de Cibersegurança (2024). Relatório de Cibersegurança em Portugal. *Riscos & Conflitos*, 5ª edição. Lisboa.

Comissão Europeia (2020). Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança. Bruxelas: Comissão Europeia. https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_pt?filename=commission-white-paper-artificial-intelligence-feb2020_pt.pdf

Elias, L. (2024). A Atuação Policial numa Nova Era Digital. In T. Rodrigues e J. Esteves (Coords.), *Preparar o Futuro: A Transição Digital na Segurança e Defesa* (1.ªed., pp. 173 – 199). Fronteira do Caos Editores.

Faqir, R. (2023). Digital Criminal Investigations in the Era of Artificial Intelligence: A Comprehensive Overview. *International Journal of Cyber Criminology*, Vol 17, 77 – 94.

Fernandez-Basso, C., Gutiérrez-Batista, K., Gómez-Romero, J., Ruiz, M. D., & Martin-Bautista, M. J. (2024). An AI knowledge-based system for police assistance in crime investigation. *Expert Systems*, e13524. https://doi.org/10.1111/exsy.13524

Fontes, J. (2022). Prevenção, policiamento e segurança – Desafios para o estado de direito democrático. *I Congresso Internacional JusCrim – Prevenção, policiamento e segurança: implicações nos direitos humanos*, pp 133 – 139. Escola de Direito da Universidade do Minho.

Gund, P., Patil, S., Phalke, V. (2023). Investigating Crime: A Role of Artificial Intelligence in Criminal Justice. *The Online Journal Of Distance Educational and e.Learning*, Volume 11, 1520 – 1526.

Kissinger, H., Schmidt, E., Huttenlocher, D. (2021). *A Era da Inteligência Artificial* (6.ª ed.). Publicações Dom Quixote.

Lanceiro, R. (2024). Artificial Intelligence and Public Administration: The problems and possible answers by the AI Act. Lisbon Public Law, Working Paper Series No 2024 – 3.

Lourenço, M. (2024). Um novo olhar sobre velhos saberes: os préstimos da inteligência artificial para a datiloscopia. *Julgar Online*, 1 – 19.

Magrani, E., & Silva, P. (2022). The Ethical na Legal Challenges of Recommender Systems Driven by Artificial Intelligence. In H. Antunes, P. Freitas, A. Oliveira, C. Pereira, E. Sequeira e L. Xavier (Eds.), *Multidisciplinary Perspectives on Artificial Intelligence and the Law* (141 – 168). Universidade Católica Portuguesa. https://doi.org/10.1007/978-3-031-41264-6

Martins, J. (2022). Inteligência Artificial e Direito: Uma Brevíssima Introdução. *Revista da Faculdade de Direito da Universidade de Lisboa*, Vol. LXIII, 1 e 2, pp. 487-506.

Moleirinho, P., Baraças, B., Augusto, R. (2024). Os Modelos Preditivos de Segurança Pública – A Aplicação da Inteligência Artificial. In T. Rodrigues e J. Esteves (Coords.), *Preparar o Futuro: A Transição Digital na Segurança e Defesa* (1.ªed., 201–226). Fronteira do Caos Editores.

Neves, L. (2024). As Transformações na Investigação Criminal. In T. Rodrigues e J. Esteves (Coords.), *Preparar o Futuro: A Transição Digital na Segurança e Defesa* (1.ªed., 227 – 254). Fronteira do Caos Editores.

Noronha, H. (2022). Prevenção, policiamento e segurança – Desafios para o estado de direito democrático. *I Congresso Internacional JusCrim – Prevenção, policiamento e segurança: implicações nos direitos humanos*, 01 – 08. Escola de Direito da Universidade do Minho.

Novais, P. (2023). Como está a Inteligência Artificial a Revolucionar o Direito: Um Caminho sem Retorno. *Colóquios do Supremo Tribunal de Justiça – Tribunais e Inteligência Artificial: Uma Odisseia no Século XXI*, 38 – 47. Supremo Tribunal de Justiça.

Nunes, R., Ricou, M., Godinho, I. & Neves, M. (2024). Inteligência Artificial (IA): Inquietações Sociais, Propostas Éticas e Orientações Políticas. https://www.cnecv.pt/pt/publicacoes/monografias/livro-branco-inteligencia-artificial-ai-inquietacoes-sociais-pro

Parlamento Europeu. (2020). O que é a inteligência artificial e como funciona?. https://www.europarl.europa.eu/topics/pt/article/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona

Piton, A. (2024). Inteligência Artificial e Reconhecimento Facial: Novas Fronteiras Penais?. In M. Valente (Coord.), *Ciências Criminais e Inteligência Artificial* (77-89). Edições Almedina.

Polícia Judiciária. (2024). Projetos Financidados – DARLENE. https://www.policiajudiciaria.pt/projetos-financiados/darlene/

Proença, L. (2023). Inteligência artificial na segurança: um desafio ou uma inevitabilidade?. In J. Pombeiro e M. Bello (Coords.), *88 Vozes Sobre a Inteligência Artificial* (1.ª ed., pp. 438 – 456). Associação Indeg Projectos ISCTE e Oficina do Livro.

Ramos, A. (2023). A IA e a sua aplicação na investigação criminal: contributo para a identificação de perfis na criminalidade organizada. Anatomia do Crime, 17, 159 – 168.

Ramos, A. (2024, novembro 11). A Inteligência Artificial aplicada à Investigação Criminal [Apresentação oral]. Curso Internacional de Estudos de Segurança Interna, Lisboa, Portugal.

Raposo, V. (2023). The Use of Facial Recognition Tecnology by Law Enforcement in Europe: a Non -Orwellian Draft Proposal. *European Journal on Criminal Policy and Research*, 29, 515 – 533. https://doi.org/10.1007/s10610-022-09512-y

Rigano, C. (2019). Using Artificial Intelligence to address criminal justice needs. *NIJ Journal*, 280, 1 – 10. Disponível em: https:// www.nij.gov/journals/280/Pages/using-artificial-intelligence-to-address-criminal-justice-needs.aspx.

Santos, A. (2023). Investigação Criminal e a Inteligência Artificial: magia digital ou uma miragem?. *Revista do Ministério Público*, 175, 207 – 221.

Smith, M. & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & Society*, 17, pp. 167 – 175. https://doi.org/10.1007/s00146-021-01199-9

Sousa, S. (2024, novembro 11). Regulamento de Inteligência Artificial da UE: Implicações de Segurança. [Apresentação oral]. Curso Internacional de Estudos de Segurança Interna, Lisboa, Portugal.

Valente, M. (2024). A utilização de robots na guerra: A responsabilidade penal. In M. Valente (Coord.), *Ciências Criminais e Inteligência Artificial* (11-27). Edições Almedina.

Legislação

Convenção Europeia dos Direitos Humanos (1950). Conselho da Europa. https://www.echr.coe.int/documents/convention_por.pdf

Declaração Universal dos Direitos Humanos (1948). Assembleia Geral das Nações Unidas. https://dre.pt/declaracao-universal-dos-direitos-humanos

Decreto de Aprovação da Constituição, de 10 de abril. Diário da República n.º 86/1976, Série I. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-aprovacao-constituicao/1976-34520775-43894075

Lei n.º 49/2008, de 27 de agosto. Diário da República n.º 165/2008, Série I. Assembleia da República. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2008-67191210-67192945

Lei n.º 53/2008, de 29 de agosto. Diário da República n.º 167/2008, Série I. Assembleia da República. https://diariodarepublica.pt/dr/legislacao-consolidada/lei/2008-34501675-108311212

Parlamento Europeu e Conselho da União Europeia. (2024). Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 que cria regras harmonizadas em matéria de inteligência artificial. Jornal Oficial da União Europeia, Série L, [p. 1 – 144]. http://data.europa.eu/eli/reg/2024/1689/oj

ESTUDO 8 – A COMUNICAÇÃO EM SITUAÇÕES DE CRISE NAS FORÇAS DE SEGURANÇA

CRISIS COMMUNICATION IN SECURITY FORCES

João Daniel Frutuoso Lourenço
Capitão GNR

RESUMO

O atual escrutínio público e atenção negativa dirigido à atuação da polícia, exponenciado pelas redes sociais ou dos *media*, aumentou a vigilância sobre as polícias. O presente artigo tem como propósito, compreender de que modo a comunicação em situações de crise pode influenciar a perceção de legitimidade de atuação pelos próprios polícias. Realizou-se uma análise bibliográfica relativa a estratégias de comunicação de crise e abordaram-se dois estudos de caso mediáticos, na Guarda Nacional Republicana e na Polícia de Segurança Pública, que permitiram analisar e explorar a resposta institucional e o seu efeito mediático. Conclui-se que a comunicação em situações de crise desempenha um papel relevante para garantir o posicionamento das forças de segurança na esfera pública. O intenso escrutínio mediático, alimentado por diversos *stakeholders*, pode afetar a legitimidade de atuação policial, pelo que se destaca a necessidade de uma comunicação de crise na perspetiva interna mais eficaz e recomenda-se uma mensagem defensiva, humanista e o reforço do apoio político às forças de segurança.

Palavras-chave: Escrutínio mediático; Comunicação de crise; legitimidade policial.

ABSTRACT

The current public scrutiny and negative attention directed at the actions of the police, exacerbated by social networks and the media, has increased vigilance over the police. The purpose of this article is to understand how communication in crisis situations can influence police officers' perception of the legitimacy of their actions. A bibliographical analysis was carried out on crisis communication strategies and two media case studies were examined, on the National Republican Guard and the Public Security Police, which allowed the institutional response and its media effect to be analysed and explored. The conclusion is that communication in crisis situations plays an important role in guaranteeing the positioning of the security forces in the public sphere. Intense media scrutiny, fuelled by various stakeholders, can affect the legitimacy of police action, which is why we highlight the need for more effective internal crisis

communication and recommend a defensive, humanist message and strengthening political support for the security forces.

***Keywords**: Media scrutiny; crisis communication; police legitimacy.*

1. INTRODUÇÃO

Muitas das mudanças nas filosofias de policiamento, quer nos EUA, quer noutros países europeus, foram impulsionadas pela indignação pública devido ao comportamento dos polícias, como casos de violência e mortes amplamente divulgadas (Nix & Wolfe, 2017).

O atual ambiente de escrutínio e atenção negativa dirigida à atuação da polícia, quer por recurso aos telemóveis quer pelos *media*, juntamente com o descontentamento crescente face ao modo de tratar as minorias, aumentou a vigilância pública sobre a polícia, sendo que, a falta de cooperação do público pode dar aos polícias uma sensação de menor segurança, contribuindo para a sua perceção de perigo, inibindo-os de atuar (Gau et al., 2024).

As alegações de parcialidade policial e uso excessivo da força em determinadas atuações policiais, em particular, perante grupos marginalizados, são ampliados pelos *media* e resultam num intenso escrutínio da polícia, podendo ocorrer um fenómeno de "*despoliciamento*", uma vez que a polícia se torna menos proativa, temendo repercussões diversas, priorizando a sua segurança, evitando o uso da força quando necessário e aumentando a renitência na abordagem a suspeitos (Wuestewald, 2022).

Face ao referido, o recurso ao uso da força policial, é normalmente conduzido para esfera pública, onde a evolução tecnológica e digital aumentou a visibilidade da atuação das forças de segurança e contribuiu para um escrutínio e criticismo contínuo, onde, sem se dar conta, está a decorrer o debate público sobre as políticas públicas que importam na sociedade (Gilardi et al., 2022). Considera-se assim, que as forças de segurança enfrentam um desafio comunicacional constante face à exposição do seu *modus operandi* perante a opinião pública, o que pode ter consequências, na reputação da instituição e influenciar o seu desempenho.

Através deste enquadramento, o presente trabalho visa explorar de que forma as estratégias de comunicação de crise adotadas pelas forças de segurança influenciam a perceção da sua própria legitimidade, tendo como principal objetivo compreender de que modo a comunicação em situações de crises policiais

mediáticas pode influenciar a atuação policial das forças de segurança, em Portugal.

Neste contexto e, de modo a articular o construto teórico dos elementos-chave, conforme indicado por Foss & Waters (2016), pretende abordar-se e debater-se no presente trabalho a seguinte questão central: "a comunicação em situações de crise policiais mediáticas influência a atuação policial das forças de segurança em Portugal?"

Para procurar dar resposta à questão central, recorreu-se à metodologia qualitativa, através da abordagem de dois estudos de caso, uma vez que a definição clara e inicial dos limites é fundamental para direcionar a atenção necessária e permitir a recolha detalhada que conduza a interpretações e conclusões enriquecidas (Njie & Asimiran, 2014). Para além disso, recorreu-se ao *clipping* de notícias, para analisar a forma como foi desenvolvida a comunicação no âmbito de duas situações de crise referentes à atuação da Guarda Nacional Republicana (GNR) e da Polícia de Segurança Pública (PSP). Considerando que esta metodologia deriva de uma combinação de características, incluindo a sua natureza sistemática, abordagem quantitativa, alta flexibilidade e adaptabilidade, poderá revelar tendências e padrões na grande maioria das comunicações, sendo um método propício e central em modelos de pesquisa e teorias da comunicação (Hansen & Machin, 2019).

O trabalho encontra-se organizado da seguinte forma: na introdução, enquadrou-se a pertinência e atualidade do tema, delineando a questão central que guia o trabalho e a metodologia aplicada; seguiu-se o enquadramento geral e conceptual para permitir compreender a temática abordada; posteriormente, aprofundaram-se os temas centrais da problemática, nomeadamente, a comunicação de crise e a influência da comunicação na atuação policial em situações de crise, apresentaram-se e discutiram-se dois casos mediáticos diferentes nas forças de segurança e teceram-se as conclusões e recomendações.

2. DA POLÍTICA PÚBLICA À COMUNICAÇÃO

De acordo com Correia e Duque (2011) o processo de emergência das políticas públicas de segurança constitui um enorme desafio para o Estado, na transformação dos ideais sociológicos e na forma como este perceciona a segurança dos cidadãos e da sociedade. Considera igualmente um desafio para as forças de segurança, que serão pressionadas pelo desencadeamento de necessidades sociais emergentes, de se desprender de modelos tradicionais de polícia de modo a adaptar-se às mudanças e pressões políticas.

Apesar das diferentes perspetivas sobre o conceito de políticas púbicas, importa adotar uma abordagem, porque para muitos académicos, definir o que entendemos por política pública ajuda a definir o seu próprio papel na formulação de políticas, assim como para as organizações (Birkland, 2019). Neste contexto, considera-se, políticas públicas, como *"o sistema de decisões públicas que visa as ações ou omissões, preventivas ou corretivas, destinadas a manter ou modificar a realidade de um ou vários setores da vida social, por meio da definição de objetivos e estratégias de atuação e da alocação dos recursos necessários para atingir os objetivos estabelecidos* (Saravia & Ferrarezi, 2006 p. 29). Birkland (2019) traz algumas ideias chave que importam referir, pois argumenta que a política pública é criada em resposta a um tipo de problema que merece algum tipo de resposta do governo, sendo orientada para um objetivo ou estado desejado, como reduzir a incidência ou a gravidade de algum tipo de problema, tendo o objetivo de alcançar resultados que permitam trazer benefício para a sociedade.

2.1. A problemática na formação de agenda e esfera pública

A esfera pública, conforme defendido por Habermas, é uma arena onde pessoas privadas se reúnem como um público para discutir tópicos de importância social e política, funcionando como um canal de comunicação entre a sociedade democrática e os atores políticos. Essencial para proteger as liberdades civis na democracia, a esfera pública inclui a imprensa, fóruns públicos, escolas e bibliotecas, mediando entre os direitos individuais e o poder do Estado (Burnett & Jaeger, 2008). Segundo Barros (2015) a esfera pública é um processo contínuo de discussão pública entre cidadãos em espaços públicos, mediado entre a sociedade e o Estado. Na sequência do pensamento de Habermas, mas numa perspetiva mais contemporânea, Seeliger & Sevignani (2022) defendem uma terceira transformação estrutural da esfera pública, impulsionada pela digitalização, mercantilização e globalização, que está a alterar profundamente as dinâmicas de decisão e formação de opinião. Essas mudanças geram uma tensão entre a pluralização das vozes públicas e a desintegração e polarização das esferas públicas (Seeliger & Sevignani, 2022), que como Innerarity (2015) defende, contribui para a desconfiança dos cidadãos e enfraquece a política e a democracia.

Outra temática importante para abordar no presente trabalho é a *agenda-setting*, que consiste no mecanismo pelo qual problemas e soluções alternativas

ganham ou perdem a atenção pública e das elites (Fischer et al., 2017). A competição entre grupos para definir a agenda é intensa, pois nenhuma sociedade ou instituição política pode lidar com todas as alternativas e problemas possíveis ao mesmo tempo. A definição de agenda envolve um conjunto de problemas, causas, símbolos, soluções e outros elementos de questões públicas que chegam à atenção do público e das entidades governamentais (Fischer et al., 2017). De acordo com Rua (2009, p. 61) a agenda de políticas públicas é uma lista de prioridades estabelecida pelos governos para direcionar os seus esforços e atenções. Essas prioridades podem mudar ao longo do tempo, dependendo da dinâmica política. Os atores políticos lutam para incluir os seus interesses nessa lista, visando torná-los objeto de decisão política.

A abordagem sobre a definição de agenda não se foca apenas nas opiniões sobre as questões em si, mas sim no seu relevo ou destaque. Os *media* têm um papel crucial na determinação sobre quais as questões em que o público deve refletir. Esse impacto dos *media* na agenda pública significa que o relevo das questões nos media influencia diretamente o seu destaque para o debate público em geral, evidenciando a ligação entre a agenda dos *media* e a agenda pública (Soroka et al., 2002).

Conforme argumenta Rua (2009), para que uma situação ou estado de coisas se torne um problema político e passe a configurar como um item prioritário da agenda governamental é necessário que apresente, pelo menos, uma das seguintes características: mobilize a ação política organizada, constitua uma situação de crise, constitua uma situação de oportunidade.

2.2. Os atores intervenientes na comunicação

Relativamente aos atores intervenientes, importa referir que as organizações contemporâneas estão cada vez mais conscientes de que precisam comunicar com os seus *stakeholders* para desenvolver e proteger a sua reputação (Cornelissen, 2014). O termo "*stakeholders*" refere-se aos portadores de interesses que serão afetados pelas decisões finais (Rua, 2009), ou *"uma pessoa ou grupo que é afetado ou pode afetar uma organização"* (Coombs, 2021b p. 4). De acordo com Cornelissen (2014) todos os grupos com interesses legítimos na organização devem ser considerados igualmente: desde o governo, grupos políticos, comunidades, aos colaboradores. As relações são interdependentes e bidirecionais, reconhecendo que os *stakeholders* tanto podem ser afetados pela organização como afetá-la. Reconhecem-se as dependências mútuas entre as organizações e os vários

grupos, que podem ser afetados pelas operações da organização, mas também podem afetar a organização, nas suas operações e desempenho, através de relações interdependentes e bidirecionais (Cornelissen, 2014). De acordo com o manual de Rua (2009), os atores nas políticas públicas, também conhecidos como "*stakeholders*", são os participantes cujos interesses serão afetados pelas decisões e ações no processo político. Eles variam de acordo com cada área de política pública e possuem recursos de poder próprios para influenciar as decisões.

3. A IMPORTÂNCIA DA COMUNICAÇÃO DE CRISE

3.1. Comunicação de crise

A comunicação de crise tem vindo a evoluir ao longo das últimas décadas. Numa primeira abordagem, as pesquisas focaram-se em definir em que consistia; numa segunda abordagem, focaram-se na organização e na sua resposta à crise e; numa terceira abordagem, focaram-se no estudo do *stakeholder*, o qual tem tentado ir ao encontro das expetativas dos colaboradores (Lawson, 2020). A resposta à crise é concebida para diminuir os danos que uma crise inflige às partes interessadas e à organização, minimizando a perturbação que uma crise pode criar (Coombs, 2021a). Tem ainda como funções: reduzir a incerteza, prestar informações e interpretações, alertas, avisos de evacuação, retirada de produtos, coordenação com os *stakeholders* chave e agências, difusão de informações e promover a ambiguidade estratégica (Sellnow & Seeger, 2021).

Para abordar a comunicação de crise, importa necessariamente compreender o que se entende por crise. De modo mais abrangente e compreensivo, pode considerar-se a crise como um *"acontecimento ou uma série de acontecimentos específicos, inesperados e não rotineiros que criam elevados níveis de incerteza e ameaçam os objetivos de alta prioridade de uma organização"* (Seeger et al., 1998, p.233). Numa perspetiva mais recente, Coombs (2021b), defende que existem três tipos de crise, designadamente: desastre, crise de saúde pública e crise organizacional. Considerando a última, que importa no presente trabalho, (Coombs, 2021b, p.3), entende que *"uma crise é a violação percebida das expectativas salientes das partes interessadas que pode criar resultados negativos para as partes interessadas e/ou para a organização"*.

Perante as várias abordagens ao conceito de crise e através da Teoria da Comunicação Situacional de Crise, Coombs faz a associação entre a crise, as suas causas e a atribuição ao nível da responsabilidade organizacional, defendendo a

existência de três tipos de crise, segundo os critérios: vítima, acidental e possível de prevenir (Coombs, 2021a).

Evidencia-se assim, a pertinência da realização desta abordagem nas forças de segurança, recorrendo-se à Teoria da Comunicação Situacional de Crise (TCSC), de modo a compreender a relação e o impacto das estratégias de resposta a crises na responsabilidade pela crise e na perceção da reputação organizacional, tendo o intuito de abordar os potenciais efeitos na auto-legitimidade dos polícias. Poder-se-á recorrer à TCSC como condutora das estratégias de resposta à crise, propondo que o capital reputacional de uma organização está refletido nas relações positivas com os seus públicos antes de uma crise, e funciona como um importante recurso durante as situações adversas (Ndone, 2023).

De acordo com Ndlela (2019), a eficácia na gestão de uma crise depende diretamente da habilidade e capacidade da organização em comunicar de forma eficiente com os seus *stakeholders* em diferentes fases da crise. Esse sucesso depende, sobretudo, da rapidez e da precisão com que as mensagens desejadas chegam aos *stakeholders* corretos. Uma comunicação bem-sucedida é essencial para que a organização preserve uma relação favorável com os seus *stakeholders* mais importantes.

3.2. Estratégias de comunicação de crise

Ndone (2023) defende várias estratégias de resposta à crise, que operam em conjunto, nomeadamente quanto à forma, fazendo referência à reconstrução; como pedidos de desculpas e compensações; e à negação, que visa excluir a responsabilidade ou atacar o acusador. Sugere, ainda, que o momento da divulgação durante uma crise é crucial para a sua gestão eficaz, pois vários investigadores têm explorado o *timing* das comunicações de crise através de duas abordagens: "*stealing thunder*" (roubar trovão) e "*thunder*" (trovão). "Stealing thunder" é uma estratégia proativa em que a organização divulga informações antes que terceiros o façam, ajudando a reduzir os danos sobre a reputação e redirecionando a atenção dos media. Por outro lado, a estratégia "*thunder*" é reativa, ou seja, espera que terceiros, como os *media*, divulguem a informação primeiro (Arpan & Pompper, 2003).

É nesse enquadramento que as forças de segurança devem ter estratégias de comunicação de crise bem definidas, pois tal como defende Ward (2014), os atores que têm a capacidade de comunicação, devem promover a inclusão e igualdade, através de iniciativas de comunicação, que permitam alcançar os

públicos e responder aos apelos da justiça. Nas respostas dadas pelas polícias em contexto destas crises, deve ir-se ao encontro da construção de uma nova ética dos novos *media* digitais, tal como defende Medina (2022), orientada para moldar a comunicação através de uma nova fórmula jornalista-comunicação-público pois, atualmente, qualquer cidadão ou instituição pode narrar uma história pelos seus meios de comunicação.

3.3. Comunicação de crise na perspetiva interna

Ao longo dos anos tem existido um grande foco na gestão de crises, dando relevo à comunicação. No entanto, existe uma lacuna na gestão de crises na perspetiva interna, sendo ainda escassos os estudos que se centram na experiência de crise dos colaboradores, motivo pelo qual, as tendências para investigação neste campo estão a focar-se na compreensão da crise centrada nos *stakeholderes* internos (Lawson, 2020), uma vez que estes são também responsáveis pelo aumento da desconfiança, queixas e frustração do público na sequência de uma crise (Almarshoodi et al., 2021). Segundo Ndone (2023), a comunicação de crise interna é uma área pouco estudada dentro do campo da comunicação de crise. O foco das investigações tem sido predominante nas dimensões externas da comunicação de crise, o que levou os investigadores a apelarem a mais investigações sobre comunicação de crise que envolvam os públicos internos ou colaboradores, com o objetivo de satisfazer a necessidade de informação durante a crise e ajudar os funcionários a lidar com ela. Argumenta, ainda, que a comunicação interna de crise desempenha um papel crucial na gestão da crise, pois defende que uma comunicação interna de crise eficaz, impede que ela se propague para os públicos externos, como os clientes, o que pode ajudar na gestão das reações dos funcionários, especialmente no que diz respeito à comunicação negativa, que pode prejudicar a reputação da organização.

A pandemia de covid 19, veio reforçar a importância da comunicação interna de crises nas organizações, revelando a necessidade de uma abordagem mais complexa do que simplesmente fornecer informações aos colaboradores externos (Heide & Simonsson, 2021). Para lidar com crises, é necessário promover a participação ativa dos colaboradores e facilitar processos de interpretação, pois só assim será possível que se constituam como "embaixadores" da organização para o público externo (Heide & Simonsson, 2021). De acordo com Mohamad et al. (2023), o envolvimento dos trabalhadores na conceção de políticas e estratégias durante as crises está a receber cada vez mais atenção devido à sua associação com

o desempenho organizacional, pois considera-se cada vez mais consolidado que os funcionários são fundamentais para a recuperação pós-crise de uma organização.

Adotar uma comunicação proativa é o primeiro passo para limitar surpresas, construir credibilidade e garantir confiança. Para tal, é fundamental criar uma narrativa uniforme e consistente para partilhar com todos os *stakeholders*, disponibilizando a verdade para evitar discrepâncias e garantir informação credível e consistente (Ndlela, 2019).

De acordo com Ndlela (2019) é importante incluir os colaboradores no esforço de comunicação já que atuam como representantes de uma empresa, constituindo-se como uma importante primeira linha de defesa para com os clientes. Ndlela (2019) indica que a comunicação com os funcionários devem incluir uma descrição aberta e clara sobre a situação, os passos que estão a ser tomados para resolver os problemas e uma visão positiva do potencial da empresa. Envolver *stakeholders* internos, como os funcionários, contribui para erradicar rumores imprecisos e abordar questões que afetam diretamente os colaboradores. Os *stakeholders* devem receber informações que os ajudem a entender a posição da organização e chegar a uma conclusão consensual.

4. O MEDIATISMO E A ATIVIDADE POLICIAL

4.1. A DISCRIMINAÇÃO POLICIAL

O relatório anual do *Institute for Crisis Management* apresenta a cobertura noticiosa de crises empresariais em 2023, onde elenca várias categorias de crise (ICM, 2024). De entre catástrofes; ativismo dos consumidores; cibercrime, entre outras, a discriminação é uma das categorias mencionadas, representando 7% das crises, sendo considerada a mais relevante para o presente trabalho. Apesar de não se encontrarem dados relativos a situações de crise nas forças de segurança, considera-se que as situações relacionadas com alegada discriminação na atuação policial serão as que mais poderão gerar uma situação de crise nas forças de segurança (Kogan et al., 2024; Rossler & Scheer, 2024).

Após o homicídio de George Floyd, em maio de 2020, o movimento "*Black Lives Matter*" veio destacar ainda mais o escrutínio público e mediático existente sobre a atuação policial, não só nos Estados Unidos da América, mas também na Europa, focando-se essencialmente no tratamento agressivo ou na violência policial que é usada, em particular, sobre minorias ou migrantes (Kogan et al., 2024; Rossler & Scheer, 2024). As situações de discriminação policial, em particular, sobre

migrantes, estão associadas a uma maior desconfiança das instituições policiais e de justiça, dificultando não só a atuação policial, mas também a integração social (Kogan et al., 2024). No entanto, poucos têm sido os estudos que se debruçam sobre o impacto e influência das situações de atuação da polícia na perspetiva interna (Rossler & Scheer, 2024).

4.2. A expetativa de confiança

Conforme argumenta Schaap (2021), que refere que as estratégias de criação de confiança se desenvolvem num complexo, imprevisível e dinâmico contexto de fatores sociais e institucionais inter-relacionados, e conclui que as estratégias de criação de confiança são moldadas por características nacionais e culturais muitas vezes únicas (Schaap, 2021), as organizações devem pautar pela igualdade que promove o capital social, tal como a confiança, honestidade, cooperação e reforço das instituições (Borzino et al., 2023). De realçar que a importância da formação cultural para assegurar o relacionamento da polícia com minorias é relevante para construir a confiança, podendo ser assegurado através de uma comunicação eficaz (Asllani & Fisher, 2021).

É de acordo com este pensamento e focado no reforço das instituições, que se optou pela abordagem sobre a perceção da auto-legitimidade, no sentido de compreender a perspetiva interna da instituição perante situações de crise.

4.3. A legitimidade policial

A legitimidade da atividade policial encontra-se normalmente associada à forma de garantir o cumprimento das normas legais, mas vários estudos têm vindo a sugerir que a lei, por si só, não garante essa legitimidade (Reising & Robert, 2014). A legitimidade é tradicionalmente vista do ponto de vista dos cidadãos, sendo que, essa perceção sobre a autoridade policial influência a forma como os polícias veem o seu poder de atuação (Wuestewald, 2022). Por outro lado, a forma como os polícias percecionam o apoio do público interfere na motivação e desempenho dos polícias e pode influenciar a sua disposição para agir proactivamente perante problemas comunitários e na aplicação da lei (Nix & Wolfe, 2017).

A relação do público com a polícia tende a ser positiva, especialmente quando existe uma estratégia de relações públicas eficaz, no entanto, é normal que surjam críticas quando a atuação policial é vista de forma excessiva ou inadequada perante certas situações, ou quando se suspeita de preconceitos racistas (Duarte,

2020). Quando este tipo de enquadramento é acompanhado e seguido pelos *media*, poderá ampliar o efeito negativo e gerar uma reprovação pública. Esta, uma vez direcionada à própria organização policial, pode resultar numa crise de legitimidade e afetar a confiança mútua, uma vez que as exigências e revindicações da legitimidade do público multiplicam-se, em particular através das redes sociais (Duarte, 2020; Czudnochowski & Ludewig, 2023).

As reações à publicidade negativa variam conforme o contexto social dos indivíduos, mas, entre os próprios polícias, esta cobertura pode fortalecer uma visão de "nós contra eles" levando à desmotivação e insegurança quanto ao apoio público e, potencialmente, à ineficácia na execução das suas funções (Duarte, 2020).

De acordo com Tyler (2007), a legitimidade centra-se na confiança e justiça processual, porque as pessoas valorizam a equidade nos processos sociais, o que influencia a sua opinião sobre instituições, como a polícia. No caso da Alemanha, quando ocorrem situações que geram críticas à atuação policial individual, a confiança da maioria na polícia mantém-se elevada, uma vez que a polícia é tradicionalmente vista como uma autoridade legítima da ordem, mas que depende do apoio e da cooperação voluntária da população para cumprir as suas tarefas (Czudnochowski & Ludewig, 2023).

A legitimidade policial deverá ser assente nas crenças e valores comuns prevalentes na sociedade e de acordo com as avaliações públicas que lhe são feitas, devendo encontrar-se de acordo com os valores reconhecidos pela sociedade, entendendo-se como um conceito multidimensional constituído pela justiça processual, justiça distributiva, eficácia e legalidade da polícia (Reising & Robert, 2014, p. 46).

Na perspetiva interna, que tem sido pouco abordada, Tankebe (2019) argumenta que a auto-legitimidade se sustenta essencialmente em três aspetos, no clima moral, em que os polícias se sentem reconhecidos e aceites pelos seus pares; a ligação entre a auto-legitimidade e as orientações normativas em relação aos membros do público, onde os polícias que acreditam na sua própria legitimidade estão mais predispostos à justiça processual nas interações polícia-cidadão; e, por fim, o papel da eficácia na formação de orientações normativas para os cidadãos, que considera o fator preditor consistente para o compromisso com a justiça processual, da parte dos polícias. Posto isto, a auto-legitimidade, ou a confiança dos agentes na sua autoridade é prejudicada por sinais de falta de apoio público, como tumultos e manifestações e pode influenciar o comportamento dos agentes

(Wuestewald, 2022). Assim, quando os polícias têm a perceção de que a organização policial é eficaz no cumprimento da sua missão tendem, geralmente, a manifestar atitudes positivas em relação aos cidadãos (Tankebe, 2019).

De acordo com o estudo de Czudnochowski e Ludewig (2023) sobre as redes sociais e a auto-legitimidade policial, para ganhar e manter a legitimidade, devem adotar-se estratégias de divulgação da informação para combater possíveis efeitos discursivos fora do controlo da polícia, baseando-se na factualidade e na neutralidade. Para além disso, o momento e a velocidade da comunicação, bem como os aspetos da comunicação relacionados com o conteúdo, proporcionam novas oportunidades para abordar as questões numa fase precoce e para manter o controlo da informação do lado da polícia, sendo os gabinetes de comunicação, uma fonte exclusiva de informação, o que lhes permite ocupar uma posição proeminente no discurso público (Czudnochowski & Ludewig, 2023).

5. OS CASOS DE ESTUDO

Para compreender as respostas a situações de crise por parte das Forças de Segurança, decidiu-se analisar dois casos concretos que foram alvo de escrutínio público nos *media*, nomeadamente, o caso da GNR em que "*militares da GNR filmaram-se a torturar imigrantes em Odemira*" divulgado a 16 de dezembro de 2021 pela CNN (Ramos, 2021) e o caso recente da PSP, do "*suspeito de furto de viatura que morre após ser baleado pela PSP*", na Cova da Moura, a 21 de outubro de 2024 (Carneiro, 2024), pelo que foram solicitados aos porta-vozes da GNR e PSP os comunicados de imprensa.

Além disso, para compreender o escrutínio público e a sua possível influência na atuação policial, recorreu-se ao *clipping* de notícias, através da plataforma informática CISION[87] para recolher todas as notícias que abordaram o assunto e posteriormente, selecionou-se e analisou-se a informação recolhida, de modo a avaliar o impacto mediático das duas situações de crise distintas nas forças de segurança.

Com visa a limitar o conteúdo a analisar, optou-se por examinar todos os artigos noticiosos televisivos, uma vez que, apesar da ascendência do consumo de notícias através das redes sociais ser uma tendência, o meio televisivo continua a

[87] O CISION é uma empresa especializada em serviços de media *intelligence* e relações públicas.

ser o mais representativo no consumo de notícias em Portugal (Cardoso et al., 2023; Newman et al., 2023). Com vista a reduzir o número elevado de notícias previsto para investigar, optou-se pela análise apenas dos artigos noticiosos referentes ao dia em que se obteve conhecimento do evento de crise bem como do dia seguinte, de modo a compreender o escrutínio público realizado, o efeito das estratégias de resposta institucionais e as reações tidas pelos vários *stakeholders*.

Para analisar a perspetiva de comunicação, recorreu-se à técnica de análise categorial, como sendo o método ideal, para analisar as expressões dos artigos noticiosos relevantes para o presente trabalho (Bardin, 1977). Por forma a sistematizar o conteúdo a dissecar, efetuou-se o registo da notícia, com um número, para fácil identificação, a data, o título, o órgão de comunicação social (OCS) e o *lead* da notícia que oferece muita informação para análise que se considera adequada.

De todos os artigos noticiosos televisivos apresentados no período definido, selecionaram-se apenas aqueles que estão relacionados com o caso de Odemira, na GNR, e com o caso da morte de Odair, na PSP. Após essa seleção, foram categorizados e agrupados em dois grupos distintos, de acordo com a revisão da literatura. Um dedicado à análise do apoio à força policial, na perspetiva interna e outro dedicado à identificação do *stakeholder*.

Quanto ao primeiro, considerou-se a perspetiva de Wuestewald (2022), onde indica que a auto-legitimidade, ou a confiança dos agentes na sua autoridade é prejudicada por sinais de falta de apoio público, tendo-se considerado três grupos: A- Apoio; B- Falta de apoio; C- Neutro. Quanto à análise do *stakeholder*, seguiu-se a perspetiva de Cornelissen (2014) quanto aos atores com interesses legítimos na organização, tendo sido realizada a distinção em quatro grupos que se organizaram com a seguinte numeração: 1- governo; 2-grupos políticos, 3- comunidades e 4-colaboradores (Polícia /Instituição).

Para realizar a análise e categorização dos artigos noticiosos, foi tido em consideração o título e *lead* da notícia, pois representam o essencial da notícia televisiva em causa, sendo conjugado e analisado de acordo com os dois grupos definidos, pelo que a categorização de cada notícia foi efetuada da forma seguinte: de A1 a A4; de B1 a B4 e de C1 a C4.

6. A ANÁLISE MEDIÁTICA

Relativamente às estratégias de comunicação de crise, procedeu-se à análise dos comunicados de imprensa divulgados por cada força de segurança em cada

uma das situações. No caso da GNR, foi elaborado o comunicado de imprensa (CI) intitulado *"Esclarecimento – Acusação referente a militares do Destacamento Territorial de Odemira"* a 16 de dezembro de 2021, pelas 20H03. No caso da PSP, foi elaborado o CI intitulado *"Intervenção Policial na Amadora"* a 21 de outubro de 2024, pelas 11H59.

Atento à recolha de notícias efetuada, para a GNR, considerou-se o dia 16 e 17 de dezembro de 2021, tendo sido apresentadas um total de 1192 notícias, por sua vez e para a PSP, considerou-se o dia 21 e 22 de outubro de 2024, tendo sido disponibilizadas 1420 notícias relacionados com a PSP. Das 2612 notícias apresentadas, foram selecionadas apenas 769 que respeitam a artigos noticiosos televisivos e que se encontram relacionadas com as duas situações de crise, designadamente, 289 alusivas à situação da GNR e 480 referentes à situação da PSP que foram analisadas e categorizadas.

De acordo com o agrupamento definido e da análise efetuada às noticias foi possível identificar diversos *stakeholders*: quanto ao Governo, identificou-se como atores: o Presidente da República[88], Primeiro Ministro, Ministra da Administração Interna (MAI); quanto aos grupos políticos consideraram-se os partidos: Pessoas – Animais – Natureza (PAN), Bloco de Esquerda (BE), Partido Comunista Português (PCP), Partido Socialista (PS), Partido Social Democrata (PSD), CDS – Partido Popular e Chega; quanto à comunidade, teve-se em consideração um espectro mais alargado, nomeadamente: os *media*, comentadores, Ministério Público, Inspeção-Geral da Administração Interna (IGAI), Amnistia Internacional, Advogados, Associação de Profissionais da Guarda, Presidente da Junta de Vila Nova de Milfontes, Ex-MAI e Ex-Secretário de Estado, Associação olho vivo, a própria comunidade, ou grupo de pessoas, especialistas de segurança, SOS Racismo, Associação de moradores da Cova da Moura, Sindicato Independente dos Agentes da Polícia, Associação de moradores do Zambujal, Presidente da Câmara de Oeiras, Sobrinha de Odair, Associação Moinho da Juventude; e por último, quanto aos colaboradores, consideraram-se as intervenções institucionais da GNR e PSP.

No que se refere à avaliação do escrutínio público da atuação policial e considerando os sinais de apoio foi possível perceber, que no caso da GNR registaram-se 24 notícias de apoio, 229 de falta de apoio e 36 consideradas neutras.

[88] Não se enquadra no governo, mas representa uma figura de estado, pelo que se considerou neste grupo por associação, atendendo ao peso institucional que está inerente ao cargo.

Já no caso da PSP, registaram-se 28 notícias que revelaram apoio, 308 de falta de apoio e 144 consideradas neutras.

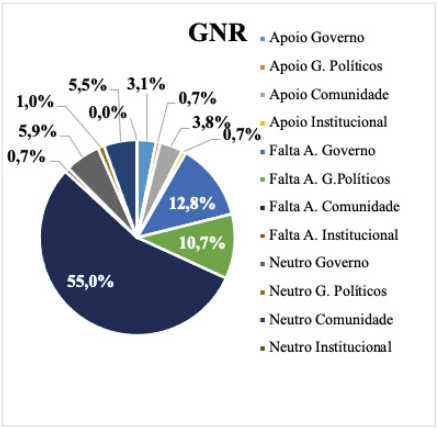

Figura 1 – Escrutínio mediático da GNR na situação de Odemira.

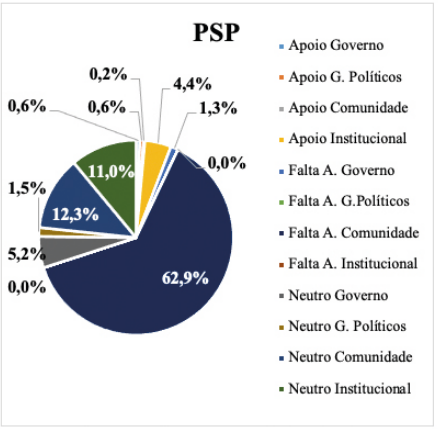

Figura 2 – Escrutínio mediático da PSP na situação de Odair.

As figuras 1 e 2 apresentam o escrutínio mediático para cada força de segurança, conjugando o *stakeholder* e os sinais de apoio. Ao verificar as mais relevantes e prestando particular atenção sobre as notícias ligadas à instituição, percebe-se que no caso da GNR, 55% das notícias são referentes à falta de apoio da comunidade, 10,7% referente à falta de apoio dos partidos e 12,8% à falta de apoio do Governo, quanto à Instituição, 1 % demonstram falta de apoio e 0,7 % demonstraram apoio. Na PSP, 62,9% das notícias são referentes à falta de apoio da comunidade, 11% referente à falta de apoio dos partidos e 12,3% à falta de apoio do Governo, quanto à Instituição, 1,5 % demonstram falta de apoio e 4,4% demonstraram apoio.

7. DISCUSSÃO

Relativamente à comunicação de crise analisaram-se os comunicados de imprensa segundo o quadro de comunicação de crise na perspetiva interna.

No caso do CI da GNR, verificou-se que foram usadas expressões como *"cumpre esclarecer", "denunciado pela própria Guarda" "prontamente reportou-os ao Ministério Público" "prestou toda a colaboração", "rigor e a transparência"* e detalharam-se aspetos relativos aos processos disciplinares desenvolvidos, o que

revela que foi tomada uma postura de proatividade e de transparência institucional de modo a reduzir incertezas e a fortalecer a reputação, tal como indica Sellnow & Seeger (2021). Foi possível verificar, também, o uso da estratégia de reconstrução defendida por Coombs (2021), pelo visível esforço da GNR em reprovar e distanciar-se dos atos discriminatórios *"compromisso de tolerância zero às diferentes formas de discriminação e desigualdades*" e em sublinhar a sua proatividade através da denúncia interna dos militares e pelas sanções disciplinares já aplicadas, bem como, com a referência a ações de formação alusivas a comportamentos discriminatórios. A GNR demonstrou, assim, o seu posicionamento institucional quanto aos atos praticados e dirigiu de forma implícita uma mensagem para os militares da GNR, não só pela referência à tolerância zero, mas também com a expressão *"os militares que servem e que já serviram a Instituição, não se reveem na conduta"*, o que, demonstra uma preocupação de incluir e envolver os seus colaboradores na perspetiva interna da comunicação, tal como argumenta Ndlela (2019) e Mohamad et al., 2023). Foi notório também a ausência de uma mensagem dirigida às vítimas, o que pode contribuir para um efeito negativo da mensagem, criando distanciamento com o público (Ndlela, 2019). Apesar da GNR já ter conhecimento dos factos, e ao reagir apenas depois da CNN lançar a notícia, enquadra-se na estratégia "*thunder*" por ser reativa. No entanto, considerando o detalhe, clareza e rapidez do comunicado, sendo divulgado pelas 20:03 horas do dia 16 de dezembro de 2021 para esclarecer a situação, mesmo antes de outros media terem avançado notícias, enquadra-se parcialmente na estratégia "*stealing thunder*", pois como defende Ndone (2023), procurou divulgar informações antes que terceiros o façam, ajudando a reduzir os danos sobre a reputação e tentando direcionar a atenção dos *media* para a transparência institucional.

No caso do CI da PSP, o comunicado focou-se em esclarecer detalhadamente as circunstâncias da atuação policial e a justificar a atuação policial, sendo feitas referências a *"quando os polícias procediam à abordagem do suspeito… terá resistido à detenção… tentado agredi-los com recurso a arma branca"* e *"esgotados outros meios e esforços"* que se enquadra no recurso ao uso de uma estratégia mista. Por um lado, a reconstrução, que reflete a abordagem adaptativa recomendada por Coombs (2021), através da TCSC para mitigar impactos reputacionais e, por outro, de negação parcial (Ndone, 2023), para diminuir ou excluir a responsabilidade pela crise. Remete ainda para o eventual apuramento de responsabilidades para um momento posterior, referindo-se a expressões como *"em circunstâncias a apurar*

em sede de inquérito criminal e disciplinar" "foi dado conhecimento ao Ministério Público e à Polícia Judiciária" o que evidenciou também transparência institucional, tal como argumenta Sellnow e Seeger (2021) demonstrando abertura para o apuramento das circunstâncias. Neste comunicado foi ainda incluído o lamentar da morte do suspeito *"…lamentavelmente e apesar da pronta assistência médica, terá falecido…" "A Polícia de Segurança Pública lamenta o desfecho deste incidente…"* e as condolências à família *"endereçando as condolências à família e amigos do cidadão falecido"* demonstrando sensibilidade, alinhando-se com a recomendação de humanizar a comunicação para melhorar a perceção pública conforme sugere Ndlela (2019).

A PSP procurou dar também uma resposta rápida e precisa conforme indica Ndlela (2019), tendo enviado o comunicado pelas 11:59 do 21 de outubro de 2024, que apesar da celeridade se enquadra na estratégia "thunder" Ndone (2023), por haver a essa hora várias notícias sobre o sucedido e por procurar dar respostas aos pedidos dos jornalistas. De realçar que a forma defensiva da atuação policial inerente ao texto do comunicado, transmitiu o posicionamento institucional sobre a situação e contribuiu para o envolvimento dos agentes da PSP (Mohamad et al., 2023) refletindo o apoio e reforço da instituição perante a perspetiva interna (Borzino et al., 2023).

Foi também interessante observar como ambas as forças de segurança, através dos seus comunicados, procuram responder a apelos da justiça como defende Ward (2014), por um lado, referindo que vão apurar circunstâncias e, por outro, demarcando-se de atitudes negativas para que, dessa forma possam alcançar os públicos.

Referente à perspetiva da auto-legitimidade policial e considerando os dados apresentados quanto à análise noticiosa, procurou-se fazer uma análise do escrutínio público e mediático que existiu sobre ambas as atuações policiais conforme realçado por Wuestewald (2022), em particular sobre as situações que envolvem migrantes e recurso ao uso da força por parte da polícia, conforme exposto por Kogan et al. (2024) e Rossler e Scheer (2024).

Torna-se também evidente a lacuna na comunicação de crise na perspetiva interna, conforme destaca Lawson (2020) e Almarshoodi et al. (2021), que é sustentada pelos dados apresentados na figura n.º 2 e n.º 3 refletindo-se numa evidência clara de falta de apoio, identificada na discussão pública (Barros, 2015) e ampliada através da tensão entre a pluralização das vozes públicas e polarização das

esferas públicas com a intervenção de vários atores políticos, tal como indicado por Seeliger e Sevignani (2022) e confirmada pelos vários *stakeholders* que intervieram no espaço mediático, em particular aqueles que se pronunciaram através de falta de apoio.

Os *media* têm um papel fundamental sobre os assuntos em que o público deve refletir, conforme sugere Soroka et al. (2002). Estas situações de crise, de acordo com Rua (2009) configuram problemas políticos e, por isso, ganham atenção pública e marcam a definição de agenda (Fischer et al., 2017), motivo pelo qual se observou a intervenção de vários atores do governo e de grupos políticos marcando, desta forma, os temas na esfera pública de modo a dar respostas a um problema político que pode influenciar as políticas públicas.

No caso da GNR, das 289 notícias analisadas, 229 (79,2%) indicaram falta de apoio em expressões exemplo, como "*O primeiro-ministro repudia as agressões a migrantes de que estão acusados 7 militares da GNR*" (notícia n.º 95), enquanto apenas 8,3% indicaram apoio. O caso da PSP enfrentou ainda um maior escrutínio mediático, dado que em 308 de 480 notícias (64,2%) refletiram falta de apoio e 5,8% demonstraram apoio, realçando várias críticas como "*A SOS Racismo exige a suspensão imediata dos agentes da PSP envolvidos na morte deste homem na Cova da Moura*" (notícia n.º 188) e a falta de apoio da comunidade local "*Pelo menos 30 pessoas causaram distúrbios no Bairro do Zambujal na Amadora, onde morava o homem que foi morto a tiro pela PSP na Cova da Moura*." (notícia n.º 32). Sem prejuízo da comunicação efetuada pelas forças de segurança, a intervenção e posicionamento político sobre a situação é fundamental, como se viu anteriormente. No entanto, a ausência de mensagens de apoio aos polícias, evidencia a dificuldade que as forças de segurança têm em gerir as situações de crise e de tentar mitigar as perceções negativas internas que afetam a perceção de legitimidade policial (Wuestewald, 2022). Para além disso, a forma como os polícias assistem à falta de apoio e de cooperação do público (Gau et al., 2024), pode interferir com a sua motivação e comprometer o seu desempenho em situações futuras (Nix & Wolfe, 2017), podendo-se assistir ao fenómeno de "despoliciamento" como refere Wuestewald (2022).

Por outro lado, mensagens que repudiam a situação, mas que reforcem a instituição tal como "*O Presidente da República diz que os imigrantes têm de ser respeitados e garante também que não deve confundir-se o todo da GNR com alguns elementos*." (notícia n.º 60) ou "*A Ministra da Administração Interna saiu em defesa*

da atuação da polícia na última noite no Bairro do Zambujal. Margarida Blasco diz que PSP limitou-se a manter a ordem pública." (notícia n.º 121) são extremamente relevantes para o apoio e reforço da instituição como indica Borzino et al., 2023 e para fortalecer a legitimidade policial e confiança dos polícias, tal como argumentam Czudnochowski e Ludewig (2023) e Tyler (2007).

Por último, importa debruçar sob o efeito dos comunicados elaborados em resposta à crise no campo mediático. Com apenas 1,4% das notícias referentes à reação da GNR, duas notícias evidenciaram apoio como "*…em comunicado, a GNR afirma que denunciou as agressões por parte de cinco elementos da Guarda Nacional Republicana" (notícia n.º 124) e duas não apoio como "e a GNR esclarece que dos 7 militares envolvidos, 2 foram suspensos*" (notícia n.º 113), pelo que o comunicado da GNR, não conseguiu equilibrar as 229 notícias de falta de apoio (79,2%). Embora o comunicado tenha destacado a proatividade e transparência da instituição em denunciar os factos e a distanciar-se dos comportamentos adotados com a referência de que os militares não se reveem naquela conduta, não foi possível transpor para os media uma mensagem de apoio aos militares.

Por sua vez, no caso da PSP, cerca de 15,4% das notícias foram referentes à reação da polícia, 21 notícias (4,4%) evidenciaram apoio, tal como, "*a Polícia de Segurança Pública emitiu há instantes um comunicado, diz que reitera e que tem por missão garantir a segurança e ordem pública e o respeito pelos direitos, liberdades e garantias dos cidadãos pelo que apela à calma*" (notícia n.º 64), e 53 notícias[89] (11,28%) referem-se ao posicionamento neutro, sendo que não existem notícias por falta de apoio referente ao posicionamento da polícia. Apesar de também não conseguir equilibrar as 302 notícias (63%) de falta de apoio, é notória a expressão de apoio, que é resultado do caráter defensivo do comunicado relativo à atuação policial da PSP e que contribui para a legitimidade policial.

8. CONCLUSÕES

Em conclusão e de modo a ir ao encontro do objetivo do presente trabalho analisaram-se os comunicados da GNR e da PSP à luz das estratégias de comunicação de crise, observando a sua influência nos media; verificou-se o escrutínio mediático com a intervenção de vários stakeholders; e observaram-se

[89] De referir que 53 notícias foram consideradas como neutras, porque se referiram a pontos de situação sobre os desacatos posteriores à situação inicial.

os sinais de apoio relativos à atuação policial que podem influenciar a legitimidade policial.

A análise efetuada permitiu responder à questão central e demonstrar que a comunicação em situações de crise desempenha um papel relevante para garantir o posicionamento das forças de segurança na esfera pública que tem influência sobre a perceção de auto-legimidade dos polícias.

Pese embora, se tenham abordado duas situações de crise policial distintas, que carecem de abordagens diferentes, foi possível constatar que as estratégias de comunicação de crise adotadas pela GNR e PSP tiveram pouco impacto no debate público, sendo pouco eficazes a criar apoio na perspetiva interna. Apesar do esforço institucional em seguir estratégias de comunicação de crise assentes na proatividade e transparência, apurou-se que não foi suficiente para gerar apoio aos polícias e equilibrar as intervenções negativas.

O intenso escrutínio mediático sobre ambas as atuações policiais, que ocorreu através da pluralização das vozes públicas, com a intervenção de vários *stakeholders*, como políticos, associações, os *media* e a própria comunidade, bem como com a desintegração e polarização pública, através de posições distintas, na sua generalidade em tom de crítica e demonstrando falta de apoio quanto à atuação policial, podem ter influência na auto-legitimidade policial, porque a forma como os polícias percecionam esse escrutínio e o apoio público, pode interferir com o seu desempenho e influenciar a sua disposição para atuar.

Evidenciou-se assim, que continua a existir uma lacuna na comunicação de crise direcionada para a perspetiva interna através do debate na esfera pública, sendo claramente demonstrado que os *media* determinam a amplificação pública negativa da atuação policial que pode afetar os polícias, pelo que, com efeito, recomenda-se o seguinte:

- A adotação de uma mensagem defensiva da instituição na estratégia de resposta à crise, direcionada para a perspetiva interna, de modo a envolver os polícias.
- Aprofundar a sensibilidade das respostas a crises, numa perspetiva mais humanista, para alcançar o apoio, cooperação e confiança do público.

Os atores políticos, em particular do governo, devem adotar um posicionamento equilibrado, mas reforçar os sinais de apoio às forças de segurança.

REFERÊNCIAS BIBLIOGRÁFICAS

Almarshoodi, S., Alkaabi, A., Almarashda, A., & Alkaabi, M. (2021). A model of factors influencing the implementation of artificial intelligence in crisis management: A case study of National Crisis and Emergency Management Authority (NCEMA). *International Journal of Sustainable Construction Engineering and Technology, 12*(4), 1–13. https://penerbit.uthm.edu.my/ojs/index.php/IJSCET/article/download/16032/6098

Arpan, L. M., & Pompper, D. (2003). Stormy weather: testing "stealing thunder" as a crisis communication strategy to improve communication flow between organizations and journalists. *Public Relations Review, 29*(3), 291–308. https://doi.org/10.1016/S0363-8111(03)00043-2.

Asllani, H., & Fisher, J. R. (2021). Cultural Implications of a Study of Police Communication With Minorities. *Journal of Business Diversity, 21*(3). https://doi.org/10.33423/JBD.V21I3.4429.

Bardin, L. (1977). *Análise de conteúdo*. Edições 70.

Barros, S. (2015). *Civic media functions inside the public sphere model*. MIT Center for Civic Media. https://www.researchgate.net/publication/283708206_Civic_media_functions_inside_the_public_sphere_model

Birkland, T. A. (2019). An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making: Fifth Edition. *An Introduction to the Policy Process: Theories, Concepts, and Models of Public Policy Making: Fifth Edition*, 1–413. https://doi.org/10.4324/9781351023948/INTRODUCTION-POLICY-PROCESS-THOMAS-BIRKLAND.

Borzino, N., Fatas, E., & Peterle, E. (2023). In transparency we trust an experimental study of reputation, transparency, and signaling. *Journal of Behavioral and Experimental Economics, 106*. https://doi.org/10.1016/j.socec.2023.102061.

Burnett, G., & Jaeger, P. T. (2008). Small Worlds, Lifeworlds, and Information: The Ramifications of the Information Behaviour of Social Groups in Public Policy and the Public Sphere. *Information Research: An International Electronic Journal, 13*(2).

Cardoso, G., Baldi, V., Couraceiro, P., Vasconcelos, A., & Paisana, M. (2023). *Públicos e mercados de media 2023*. www.obercom.pt.

Carneiro, C. (2024, October). *Cova da Moura. Suspeito de furto de viatura morre após ser baleado pela PSP*. https://www.dn.pt/3380342842/cova-da-moura-suspeito-de-furto-de-viatura-morre-apos-ser-baleado-pela-psp/.

Coombs, W. T. (2021a). Crisis Communication as Course Correction: Communicative Efforts Revive Goals. In *Strategic Communication in Context: Theoretical Debates and Applied Research* (pp. 111–130). UMinho Editora/CECS. https://doi.org/10.21814/uminho.ed.46.6.

Coombs, W. T. (2021b). *Ongoing Crisis Communication* (6.a). Sage.

Cornelissen, J. P. (2014). *Corporate communication : a guide to theory & practice* (4 Ed.). SAGE Publications Ltd.

Correia, E. P., & Duque, R. (2011). O poder político e a emergência das políticas públicas de segurança. *Politeia*, 8, 39–50.

Czudnochowski, D., & Ludewig, F. (2023). A driving force, a driven force? Social media and police self-legitimacy. *Https://Doi.Org/10.1177/14613557231173499, 25*(3), 226–236. https://doi.org/10.1177/14613557231173499.

Duarte, R. F. C. (2020). *Autolegitimidade policial: O impacto da publicidade negativa da atividade policial pelos mass media*. Instituto Superior de Ciências Policiais e Segurança Interna.

Fischer, F., Miller, G. J., & Sidney, M. S. (2017). Handbook of Public Policy Analysis: Theory, Politics, and Methods. In *Routledge*. https://books.google.pt/books?hl=pt-PT&lr=&id=oh03DwAAQBAJ&oi=fnd&pg=PP16&dq=handbook+of+public+policy+analysis&ots=_y1HCcTfhW&sig=KwinbVWeLO5CsxO5C7E2YNSwlro&redir_esc=y#v=onepage&q=handbook%20of%20public%20policy%20analysis&f=false.

Foss, S. K., & Waters, W. (2016). *Destination Dissertation: A Traveler's Guide to a Done Dissertation* (2.a). Rowman & Littlefield.

Gau, J. M., Roman, K. L., & Paoline, E. A. (2024). Negative publicity, citizen cooperation, and officers' perceptions of danger in the occupational environment. *Police Practice and Research, 25*(4), 387–400. https://doi.org/10.1080/15614263.2023.2268788

Gilardi, F., Gessler, T., Kubli, M., & Müller, S. (2022). Social Media and Political Agenda Setting. *Political Communication, 39*(1), 39–60. https://doi.org/10.1080/10584609.2021.1910390.

Hansen, A., & Machin, D. (2019). *Media and Communication Research Methods* (2.a). Macmillan internacional, Red Globe Press.

Heide, M., & Simonsson, C. (2021). What was that all about? On internal crisis communication and communicative coworkership during a pandemic.

Journal of Communication Management, 25(3), 256–275. https://doi.org/10.1108/JCOM-09-2020-0105/FULL/PDF.

ICM. (2024). *Annual Crisis Report 2023*.

Innerarity, Daniel. (2015). *La política en tiempos de indignación*. Galaxia Gutenberg.

Kogan, I., Weißmann, M., & Dollmann, J. (2024). Police discrimination and police distrust among ethnic minority adolescents in Germany. *Frontiers in Sociology, 9*, 1231774. https://doi.org/10.3389/FSOC.2024.1231774/BIBTEX.

Lawson, A. D. (2020). *Crisis communication - managing stakeholder relationships*. Routledge.

Medina, J. (2022). The Duties to Protest and to Listen to Protest Communicative Resistance, Enabler's Responsibility, and Echoing. *Democratic Theory, 9*(2), 101–119. https://doi.org/10.3167/dt.2022.090206.

Mohamad, B., Abbas, A., Muslim, A. &, Akanmu, D., Adamu, A. A., & Akanmu, M. D. (2023). Internal crisis communication (ICC) framework in high risk industry: A qualitative study from key informants' perspectives. *Cogent Business & Management, 10*(3). https://doi.org/10.1080/23311975.2023.2281699.

Ndlela, M. N. (2019). *Crisis Communication: A Stakeholder Approach* (Palgrave pivot, Ed.). Springer.

Ndone, J. (2023). Internal crisis communication: The effects of negative employee-organization relationships on internal reputation and employees' unsupportive behavior. *Public Relations Review, 49*(4), 102357. https://doi.org/10.1016/J.PUBREV.2023.102357.

Newman, N., Fletcher, R., Eddy, K., Robertson, C. T., & Kleis Nielsen, R. (2023). *Reuters Institute Digital News Report 2023*. https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2023.

Nix, J., & Wolfe, S. E. (2017). The Impact of Negative Publicity on Police Self-legitimacy. *Justice Quarterly, 34*(1), 84–108. https://doi.org/10.1080/07418825.2015.1102954.

Njie, B., & Asimiran, S. (2014). *Case Study as a Choice in Qualitative Methodology* (Vol. 4, Issue 3). www.iosrjournals.orgwww.iosrjournals.org.

Ramos, A. C. (2021). *Militares da GNR filmaram-se a torturar imigrantes em Odemira*. CNN.

Reising, M. D., & Robert, J. K. (2014). *The Oxford Handbook of Police and Policing* (M. D. Reisig & R. J. Kane, Eds.). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199843886.001.0001.

Rossler, M. T., & Scheer, C. (2024). Causes of Police Officer Career Apprehension Following George Floyd. *Https://Doi.Org/10.1177/10986111241234317*. https://doi.org/10.1177/10986111241234317.

Rua, M. das G. R. (2009). *Para aprender Políticas Públicas*.

Saravia, E. (organizador da coletânea), & Ferrarezi, E. (organizadora da coletânea). (2006). Coletânea de políticas públicas: volume 1: introdução à teoria da política pública. *Http://Www.Enap.Gov.Br/Index.Php?Option=com_docman&task=doc_view&gid=2857.http://repositorio.enap.gov.br/jspui/handle/1/1254*.

Schaap, D. (2021). Police trust-building strategies. A socio-institutional, comparative approach. *Policing and Society, 31*(3), 304–320. https://doi.org/10.1080/10439463.2020.1726345.

Seeger, M. W., Sellnow, T. L., & Ulmer, R. R. (1998). Communication, Organization, and Crisis. *Annals of the International Communication Association, 21*(1), 231–276. https://doi.org/10.1080/23808985.1998.11678952.

Seeliger, M., & Sevignani, S. (2022). A New Structural Transformation of the Public Sphere? An Introduction. *Https://Doi.Org/10.1177/02632764221109439, 39*(4), 3–16. https://doi.org/10.1177/02632764221109439.

Sellnow, T. L., & Seeger, M. W. (2021). *Theorizing Crisis Communication* (2.a). John Wiley & Sons.

Soroka, S. N., Blake, D., Jones, B., Jenkins, R., & Fournier, P. (2002). Issue Attributes and Agenda-Setting by Media, the Public, and Policymakers in Canada. *International Journal of Public Opinion Research, 14*(3), 264–285. https://doi.org/10.1093/IJPOR/14.3.264.

Tankebe, J. (2019). In their own eyes: an empirical examination of police self-legitimacy. *International Journal of Comparative and Applied Criminal Justice, 43*(2), 99–116. https://doi.org/10.1080/01924036.2018.1487870.

Tyler, T. R. (2007). *Legitimacy and Criminal Justice: An International Perspective* (Russel Sage Foundation, Ed.). RusselSageFoundatio.

Ward, S. J. A. (2014). Radical Media Ethics: Ethics for a global digital world. *Digital Journalism, 2*(4), 455–471. https://doi.org/10.1080/21670811.2014.952985.

Wuestewald, M. I. (2022). A legitimacy crisis? Exploring the relationships between police self-legitimacy, employee engagement, and civic engagement. *Police Practice and Research, 23*(1), 1–19. https://doi.org/10.1080/15614263.2021.1984913.

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

60 – Inteligência Artificial: Estudos Pioneiros em Contexto Militar
Coordenadora: Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

61 – Direito Internacional e Conflitos Armados: Desafios Éticos e Legais na Guerra Contemporânea
Coordenador: Tenente-coronel Pedro da Silva Monteiro

62 – Inovação e Eficiência na Administração Militar
Coordenadora: Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

63 – A Modernização das Capacidades Militares no Mundo Digital
Coordenadora: Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

64 – Forças Armadas em Transformação: Esratégias de Defesa no Mundo em Mudança
Coordenadora: Tenente-coronel Ana Carina da Costa e Silva Martins Esteves

65 – Cadernos de Saúde Militar e Medicina Operacional - Vol. II
Coordenadores: Coronel (REF) António Correia
Primeiro-tenente Nicole Esteves Correia

66 – Atas do Seminário: Poder Militar Terrestre
Coordenador: Brigadeiro-General Joaquim Manuel de Mira Branquinho

Editorial: cidium@ium.pt
Telefone: (+351) 213 002 100
Morada: Rua de Pedrouços - 1449-027 Lisboa