INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

XXXVIII CURSO DE FORMAÇÃO DE OFICIAIS DE POLÍCIA

Dissertação de Mestrado em Segurança Pública

Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal

Rodrigo Miguel Rosa Rodrigues

Aspirante a Oficial de Polícia

Orientador

Superintendente-Chefe (Doutor) Luís Manuel André Elias

Coorientadores

Superintendente-Chefe José Emanuel Matos Torres

Intendente Tito Eurico Miranda Fernandes

Lisboa, 8 de maio de 2026

INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

XXXVIII CURSO DE FORMAÇÃO DE OFICIAIS DE POLÍCIA

Dissertação de Mestrado em Segurança Pública

Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal

Rodrigo Miguel Rosa Rodrigues

Aspirante a Oficial de Polícia

Orientador

Superintendente-Chefe (Doutor) Luís Manuel André Elias

Coorientadores

Superintendente-Chefe José Emanuel Matos Torres

Intendente Tito Eurico Miranda Fernandes

Lisboa, 8 de maio de 2026

Estabelecimento de Ensino:	Instituto Superior de Ciências Policiais e Segurança Interna
Curso:	XXXVIII CFOP
Orientador:	Superintendente-Chefe (Doutor) Luís Manuel André Elias
Coorientadores:	Superintendente-Chefe José Emanuel Matos Torres Intendente Tito Eurico Miranda Fernandes
Título:	*Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal*
Autor:	Rodrigo Miguel Rosa Rodrigues
Local de Edição:	Lisboa
Data de Edição:	8 de maio de 2026

Dissertação apresentada ao Instituto Superior de Ciências Policiais e Segurança Interna com vista à obtenção do grau de Mestre em Segurança Pública, elaborada sob a orientação científica do Superintendente-Chefe (Doutor) Luís Manuel André Elias e coorientação do Superintendente-Chefe José Emanuel Matos Torres e do Intendente Tito Eurico Miranda Fernandes.

Epígrafe

"If my mind can conceive it,
if my heart can believe it,
then I can achieve it"

Muhammad Ali

Dedicatória

À minha família.

Ao meu Avô, *in memoriam*.

Agradecimentos

Chega o fim desta dura, mas bela caminhada. Apesar dos altos e baixos, sempre soube que era este o caminho que ambicionava percorrer e todo o esforço fez sentido. No entanto, nunca seria possível sem todos os que se cruzaram no meu caminho e que fazem esta viagem valer a pena.

Em primeiro, às pessoas mais importantes da minha vida, a minha família e a minha namorada. Em especial, ao meu Pai por seres a minha maior referência em tudo. À minha Mãe por prezares sempre pelo meu bem-estar, independentemente das circunstâncias. À minha Maninha pelo orgulho que me dá ver-te crescer e tornares-te alguém que nos enche de orgulho a todos. E à minha Quica, pelo amor e paz que me proporcionas, és a base que me permite ambicionar ser mais e melhor.

Sempre fiz questão de valorizar e cultivar fortes laços de amizade, em especial nesta etapa, porque isso sim é o melhor que levamos. Quero agradecer:

Aos meus camaradas e amigos dos "Bachatas" e do "Too Hot", por fazerem com que estes 5 anos valessem a pena, são amizades como as vossas que preservarei comigo dentro e fora desta casa. E ao meu grupo de amigos "acima da média" pelas importantes amizades de longa data que me moldaram também naquilo que sou hoje.

Aos meus camaradas 38.º CFOP, por me mostrarem o que a camaradagem é capaz de superar. E se agora aqui estamos é reflexo disso mesmo. Aos meus camaradas e amigos mais próximos dos restantes cursos, também as vossas amizades pretendo preservar ao longo da minha vida profissional e pessoal.

Aos meus orientadores de estágio e efetivo da 41.ª e 19.ª Esquadras, assim como da 63.ª e 61.ª Esquadras. Ao Subcomissário Borrega, pelos valores transmitidos e pela amizade que levo também comigo. E ao Subcomissário João Rodrigues, meu parceiro, e sempre um verdadeiro exemplo do que um oficial, camarada e amigo deve ser. São para mim referências de liderança e profissionalismo que levarei como exemplo na minha carreira enquanto Oficial de Polícia.

Ao meu orientador, Superintendente-Chefe Luís Elias, agradeço toda a disponibilidade, os seus conselhos e correções foram essenciais para a concretização desta dissertação. Aos meus coorientadores Superintendente-Chefe Matos Torres e Intendente Tito Fernandes por terem aceitado o meu convite e por partilharem um pouco da vossa vasta experiência. O apoio e orientação de V. Exs.ª foi fundamental para concluir esta etapa final do meu percurso académico.

Aos oficiais, docentes e efetivo do ISCPSI que me moldaram e dotaram dos valores que levo agora para a minha vida profissional e pessoal.

Ao pessoal do CSP pelos valiosos contributos para este trabalho.

Ao pessoal da Blue Line JJ por não só me dotarem de competências técnicas, mas por me mostrarem também os valores que nos unem enquanto polícias.

Ao ISCPSI que me acolheu e em 5 anos me fez crescer como profissional e como pessoa. E à PSP, a instituição que me deu propósito e a quem me comprometo servir de agora em diante.

Obrigado a todos!

Resumo

A presente dissertação propõe uma análise crítica sobre o contributo da Inteligência policial no apoio à atividade operacional da segurança pessoal, procurando compreender de que forma a produção e o tratamento da informação podem reforçar a antecipação, a avaliação do risco e a tomada de decisão no Corpo de Segurança Pessoal da PSP. Partindo do enquadramento histórico, conceptual e institucional da segurança pessoal, o estudo aprofunda o papel da inteligência policial e do policiamento orientado pelas informações como instrumentos de apoio à missão policial. Desenvolve igualmente a relação entre ameaça e risco, bem como a importância do planeamento e da cenarização na proteção de altas entidades. A investigação segue uma abordagem qualitativa, assente em análise documental, revisão bibliográfica e entrevistas semiestruturadas a polícias, com funções de cariz estratégico, mas também operacional e tático, com experiência nas áreas de segurança pessoal e inteligência policial. Com base neste percurso, a dissertação identifica algumas fragilidades no atual sistema informacional e propõe linhas de melhoria orientadas para uma maior integração de uma cultura de informações no Corpo de Segurança Pessoal. Propõem-se, assim, um conjunto de procedimentos de cariz operacional que devem ser formalizados e proporcionais ao grau de ameaça e à avaliação de risco, com vista ao reforço da eficácia da segurança de altas entidades.

Palavras-chave: inteligência policial, segurança pessoal, corpo de segurança pessoal, atividade operacional.

Abstract

This dissertation offers a critical analysis of the contribution of Police Intelligence in supporting Close Protection operational activities, seeking to understand how the production and processing of information can enhance anticipation, risk assessment, and decision-making within the Close Protection Unit of the Portuguese Police. Starting from the historical, conceptual, and institutional framework of Close Protection, the study explores the role of Police Intelligence and Intelligence-Led Policing as tools to support the police mission. It also explores the relationship between threat and risk, as well as the importance of planning and scenario development in protecting high-profile entities. The research follows a qualitative approach, based on document analysis, a literature review, and semi-structured interviews with police officers with strategic, as well as operational and tactical roles, with experience in the areas of Close Protection and Police Intelligence. Based on this analysis, the dissertation identifies certain weaknesses in the current information system and proposes lines of improvement aimed at greater integration of an information culture within the Close Protection Unit. A set of operational procedures is thus proposed, which should be formalized and proportionate to the threat level and risk assessment, to strengthen the effectiveness of high-profile entity security.

Keywords: police intelligence, close protection, close protection unit, operational activity.

Índice Geral

Índice de Figuras

Lista de Siglas, Abreviaturas e Acrónimos

AIP	Área de Interesse Permanente
CRP	Constituição da República Portuguesa
CSP	Corpo de Segurança Pessoal
CTINTEL	Canal Técnico de Inteligência Policial
DACO	Divisão de Análise e Cooperação
DIC	Departamento de Investigação Criminal
DICCI	Divisão de Investigação Criminal e Cooperação Internacional
DIP	Departamento de Informações Policiais
DPTCF	Divisão de Polícia Técnica e Ciência Forense
DSGI	Divisão de Segurança e Gestão da Informação
EEI	Elementos Essenciais de Informação
ERTE	Equipa de Reação Tática Encoberta
FSS	Forças e Serviços de Segurança
GNR	Guarda Nacional Republicana
GOSPEE	Grupo Operacional de Segurança Pessoal de Entidades Estrangeiras
GOSPEN	Grupo Operacional de Segurança Pessoal de Entidades Nacionais
GOSPMT	Grupo Operacional de Segurança Pessoal de Magistrados e Testemunhas
HUMINT	Human Intelligence
IC	Investigação Criminal
IMINT	Imagery Intelligence
ISCPSI	Instituto Superior de Ciências Policiais e Segurança Interna
LOPSP	Lei Orgânica da PSP
NEP	Norma de Execução Permanente
NIP	Núcleo de Informações Policiais
OEI	Outros Elementos de Informação
OSINT	Open Source Intelligence
PJ	Polícia Judiciária
POI	Policiamento Orientado pelas Informações
PSP	Polícia de Segurança Pública
SEI	Sistema Estratégico de Informação
SIED	Serviço de Informações Estratégicas de Defesa

SIGINT	Signals Intelligence
SIRP	Sistema de Informações da República Portuguesa
SIS	Serviço de Informações de Segurança
SO/SINTEL	Subunidades Operacionais do Sistema de Inteligência Policial da PSP
TECHINT	Technical Intelligence
UE/SINTEL	Unidade Estratégica do Sistema de Inteligência Policial da PSP
UEP	Unidade Especial de Polícia
UO/SINTEL	Unidade Operacional do Sistema de Inteligência Policial da PSP

Introdução

A atividade de segurança pessoal, enquanto ramo específico da Segurança Interna e como competência reservada da Polícia de Segurança Pública, merece a nossa especial consideração relativamente à forma como atua na sua vertente operacional. Desde cedo, há registos de violência dirigida a líderes políticos, religiosos ou militares, sendo esta encarada como uma ameaça à integridade dos indivíduos visados e com potencial de destabilizar regimes e alterar o próprio curso da história (Magalhães, 2018). Neste sentido, a segurança pessoal assume-se como um instrumento essencial de garantia da ordem e da proteção das Instituições.

Este enquadramento revela-nos a importância de se conhecer bem o protegido, permitindo adequar de forma tática e técnica os procedimentos de segurança mais eficazes. Tal ideia é desenvolvida por O´Connor (1996) quando afirma que "aqueles que têm a honra de proteger um Chefe de Estado ou Governo, são tão eficazes quanto ele, ou ela, o permitem" (p.8).

Numa vertente da Segurança Interna, enquanto atividade, esta não pode ser prosseguida sem inteligência, sendo considerada um dos principais pilares a par da prevenção, da ordem pública, da investigação criminal e da cooperação internacional (Fernandes, 2004). Em Portugal, compete ao Serviço de Informações de Segurança (SIS) determinar o grau de ameaça sobre as entidades protegidas, recorrendo a escalas padronizadas recomendadas pela União Europeia. Contudo, esta ferramenta limita-se essencialmente à quantificação da ameaça, não incorporando dimensões complementares relacionadas com os potenciais impactos na esfera pessoal do protegido, designadamente ao nível das consequências previsíveis da sua concretização. Esta lacuna impede a construção de uma avaliação integrada do risco, entendido como a projeção da ameaça sobre um determinado sujeito em função da sua exposição, contexto e vulnerabilidades específicas, aspeto que Torres (2015) considera fundamental para a elaboração de um quadro situacional verdadeiramente completo.

Neste contexto, a PSP, enquanto entidade produtora de inteligência, adotou a gestão do risco como ferramenta de apoio estratégico, operacional e tático, procurando reduzir a surpresa e a incerteza inerentes à tomada de decisão. Como refere Torres (2018) a incerteza tornou-se um dos maiores inimigos da Polícia, impondo a necessidade de gerar cenários bem estruturados e simulados que permitam antecipar ameaças e preparar medidas técnico-táticas adequadas. A inteligência policial surge, assim, como elemento central para evitar a surpresa, apoiar a decisão dos comandantes e garantir a eficácia na proteção de altas entidades (Fernandes, 2014).

Neste plano, como também sublinha Elias (2022), a Inteligência assume-se como um vetor central da atividade policial, na medida em que permite transformar informação dispersa em conhecimento útil para a decisão e para a ação, reforçando a capacidade da PSP para atuar de forma preventiva e orientada pelo risco.

Já no âmbito operacional da segurança pessoal, a articulação entre a Inteligência e proteção é crucial. Apesar de o SIS avaliar o grau de ameaça, subsiste uma lacuna significativa na disponibilização de informação prática e contextualizada às equipas que atuam no terreno (Magalhães, 2023). Desta forma, a inexistência de um órgão de articulação de inteligência, com capacidade de produzir e integrar dados provenientes de diferentes entidades nacionais e internacionais, transformando-os em informação específica e concreta, limita a capacidade de antecipação e de resposta operacional eficaz e eficiente do Corpo de Segurança Pessoal (CSP).

Face a esta lacuna, define-se como objetivo da presente dissertação analisar a aplicabilidade de uma componente de inteligência policial no apoio à atividade operacional do CSP, avaliando de que modo poderá colmatar eventuais lacunas de articulação interinstitucional, reforçar a perceção situacional e potenciar a eficácia na proteção de altas entidades. Neste sentido, recorre-se a uma abordagem qualitativa, assente em análise documental, revisão de bibliografia já existente e entrevistas semiestruturadas a polícias, com funções de cariz estratégico, mas também operacional e tático, com experiência nas áreas de segurança pessoal e inteligência policial.

A presente dissertação estrutura-se, por conseguinte, em três capítulos, que se articulam de forma progressiva e cumulativa. Num primeiro momento, contruímos uma base teórica sobre o objeto de estudo, fazendo o enquadramento necessário para compreender a evolução da segurança pessoal no plano histórico, conceptual até à consolidação do CSP na sua vertente jurídica e institucional.

O segundo capítulo aprofunda o contributo da inteligência policial para a atividade operacional, destacando o papel das Informações policiais, da gestão do risco, da cenarização e da contrainteligência na construção de uma resposta mais informada, antecipada e ajustada à incerteza.

O terceiro capítulo aprofunda, por fim, a relação entre a inteligência policial e o CSP, procurando perceber de que forma essa articulação pode ser operacionalizada na prática. Mais do que diagnosticar fragilidades, procuramos neste capítulo projetar um modelo mais consolidado de recolha e difusão de informação no seio do CSP de forma a fazer face ao atual contexto securitário crescentemente complexo e exigente.

Por fim, a presente dissertação concluir-se-á com uma síntese crítica dos principais contributos teóricos e práticos desenvolvidos, evidenciando a articulação entre o enquadramento conceptual da segurança pessoal, o papel da inteligência policial e as propostas formuladas para o reforço da componente informacional do CSP. Pretende-se, assim, sistematizar os contributos do estudo e deixar linhas de orientação úteis para a otimização de um futuro modelo de inteligência policial aplicado à segurança pessoal.

Método de Investigação

A complexidade inerente ao estudo da inteligência policial aplicada à atividade operacional da segurança pessoal impõe a adoção de um modelo metodológico capaz de apreender um fenómeno profundamente especializado, onde convergem dimensões estratégicas, operacionais e humanas. A segurança pessoal, enquanto domínio específico da Segurança Interna, envolve práticas cuja natureza sensível e técnica exige uma abordagem metodológica que permita compreender a realidade para além da superfície normativa ou procedimental. Assim, a presente investigação adota uma abordagem qualitativa de matriz descritiva e interpretativa, procurando captar significados, perceções e lógicas internas que estruturam o modo como informação, risco e decisão se articulam no seio do CSP.

Como referido por Espírito Santo (2010)**,** o método científico constitui um "caminho de investigação apropriado e validado face aos objetivos, meios e resultados esperados" (p.11), sendo esta coerência interna aquilo que legitima o conhecimento produzido. A investigação científica exige, por isso, um percurso metodológico sustentado que assegure validade epistemológica dos resultados obtidos e permita ultrapassar visões fragmentadas ou redutoras da realidade. Esta postura metodológica enquadra-se na tradição compreensiva da ciência no seu sentido lato e, em particular, das Ciências Policiais, cuja natureza interdisciplinar exige a articulação entre reflexão teórica, análise crítica e observação das próprias práticas profissionais.

A necessidade de uma rutura epistemológica com o senso comum, tal como sustenta Durkheim (2010), revela-se particularmente relevante neste contexto. A rejeição do conhecimento vulgar e das pré-noções, frequentemente marcadas por juízos ideológicos ou por experiências pessoais não sistematizadas, impõe a necessidade de uma revisão crítica da bibliografia e do estado da arte. Este movimento epistemológico permite libertar a investigação de enviesamentos cognitivos e de construções teóricas artificiais, assegurando que a problemática é formulada em termos científicos e não intuitivos. Assim, a operacionalização da pergunta de partida, centrada na pertinência de uma componente de inteligência policial no apoio à atividade operacional do CSP, ultrapassa a mera delimitação temática e configura o gesto inaugural de uma investigação rigorosa, tal como defendem Quivy & Campenhoudt, (2005). A problemática organiza-se, deste modo, em eixos analíticos que estruturam toda a estrutura teórica da dissertação, conferindo-lhe consistência argumentativa e coerência teórica.

Acresce que a pluralidade metodológica adotada, combinando análise documental, revisão bibliográfica especializada e entrevistas, reforça a robustez e a profundidade

interpretativa do estudo. A articulação entre métodos qualitativos, como a entrevista semiestruturada, e a análise sistemática de fontes secundárias permite apreender não apenas os discursos normativos e institucionais, mas também os significados que os próprios intervenientes atribuem às suas práticas. Tal como salientam Quivy & Campenhoudt, (2005), a entrevista constitui um instrumento privilegiado para captar a complexidade social, oferecendo contributos empíricos densos e matizados. Assim, para além da análise documental, recorre-se à realização de entrevistas que servirão de suporte e complemento à revisão bibliográfica desenvolvida, permitindo integrar no quadro teórico da investigação os contributos mais relevantes identificados pelos participantes.

O *corpus* empírico é constituído por entrevistas semiestruturadas, das quais cinco gravadas via videoconferência, uma gravada presencialmente e uma respondida em formulário próprio, sendo posteriormente todas transcritas na íntegra para os apêndices da presente dissertação. Estas permitem captar as representações, experiências e recomendações dos participantes, oferecendo um contributo substancial para a análise crítica e fundamentada do fenómeno em estudo. Assim, o *corpus* não se limita a funcionar como um simples repositório de informação, assumindo-se como um espaço de construção de sentido, no qual se revelam as tensões, perceções e dinâmicas que atravessam a vertente operacional e informacional associada à atividade do CSP.

A seleção dos participantes seguiu uma lógica de amostragem intencional, conforme proposto por Patton (2002), orientada para a saturação teórica e a representatividade funcional. O universo deste estudo é constituído por sete participantes, integrando quatro oficiais e três chefes da PSP, todos com experiência profissional no domínio das valências de segurança pessoal e da inteligência policial. Dada a sensibilidade das matérias abordadas nas entrevistas optou-se por manter o anonimato dos entrevistados, codificando os entrevistados como: E1, E2, E3, E4, E5, E6 e E7. A seleção deste grupo visa garantir que as perspetivas recolhidas sejam simultaneamente informadas por uma visão estratégica e por experiência operacional e tática direta no terreno, permitindo uma análise crítica das necessidades, limitações e potenciais contributos de uma componente de inteligência policial no apoio à atividade operacional do CSP. A heterogeneidade funcional e hierárquica dos participantes possibilita obter uma visão abrangente e multifacetada do objeto de estudo, confrontando perceções de nível estratégico e perceções de nível operacional e tático.

A construção de um percurso metodológico sólido e devidamente orientado constitui condição essencial para alcançar os objetivos científicos definidos nesta investigação. Por essa

razão, a formulação da pergunta de partida assume um papel estruturante, funcionando como eixo que guia toda a reflexão analítica e empírica subsequente. Tal como referem Campenhoudt et al. (2017)**,** a pergunta de partida é o instrumento mais eficaz para assegurar a coerência interna de um projeto de investigação, na medida em que permite ao investigador "exprimir o mais exatamente possível o que procura saber, elucidar, compreender melhor" (p. 42).

Assim, é com base nesta premissa epistemológica que se estrutura o presente estudo, tomando como ponto de partida a pergunta central que orienta toda a investigação. Esta visa analisar criticamente as necessidades, limitações e potencialidades associadas à criação de uma componente de inteligência policial dedicada ao apoio da atividade operacional do CSP. Consubstanciando-se na seguinte pergunta de partida: "Como poderá uma componente de inteligência policial, dedicada a apoiar a atividade operacional do CSP, potenciar a eficácia no processo de segurança de altas entidades e outras que beneficiam de segurança pessoal?".

Tendo em consideração a complexidade da problemática e a necessidade de uma abordagem multifacetada, formulam-se três questões derivadas que contribuem para uma análise mais abrangente e sustentada do fenómeno. A primeira procura compreender de que forma as lacunas de articulação com outras subunidades e entidades na partilha de inteligência policial podem comprometer a eficácia operacional do CSP. A segunda questiona em que medida a integração de uma componente de inteligência policial poderá melhorar a perceção situacional e a capacidade de resposta das equipas de segurança pessoal perante ameaças dinâmicas. Por fim, a terceira analisa a pertinência de uma atividade própria de contrainteligência e desinformação no seio do sistema informacional do CSP.

Constitui-se, deste modo, uma grelha interrogativa que permite, por um lado, identificar fragilidades existentes nos atuais fluxos informacionais e, por outro, explorar os contributos que uma componente de inteligência policial poderá oferecer no reforço da antecipação, da avaliação do risco e da tomada de decisão no contexto da segurança pessoal.

Capítulo I: Contexto e Evolução da Segurança pessoal

I.1. Conceptualização da Segurança pessoal

A segurança pessoal é tão antiga quanto o próprio exercício do poder. Ao longo da história, sempre que existiu alguém munido de soberania ou autoridade política, foi comum a presença de indivíduos especificamente incumbidos da sua proteção. Estes elementos eram criteriosamente selecionados, sobretudo em função da sua robustez física e da sua destreza no combate, sendo-lhes exigido um elevado grau de lealdade e disponibilidade para o sacrifício extremo, incluindo a entrega da própria vida, se tal se revelasse necessário (Schneider, 2005, p. 54).

A análise da segurança pessoal exige, antes de mais, um esforço de clarificação conceptual. É comum, na gíria, o emprego do epíteto "guarda-costas", ainda que se trate de um termo redutor e generalista que pouco faz justiça à complexidade técnico-operacional da atividade profissional a que corresponde a segurança pessoal. A própria diversidade terminológica que surge noutras línguas — *close protection*, *dignitary protection* ou *personal protection* em inglês, *seguridad inmediata* ou *protección de altas personalidades* em espanhol, *protection rapprochée* em francês — evidencia que estamos perante um conceito cuja precisão científica ou técnica não é uniforme e que, por isso mesmo, carece de clarificação antes de ser aprofundado (Santos, 2020).

Na literatura internacional, a segurança pessoal é geralmente entendida como uma atividade centrada na proteção de indivíduos expostos a ameaças específicas, assumindo um carácter meramente funcional e abrangente, embora nem sempre explicite os métodos e fundamentos operacionais que a estruturam. Importa ainda referir que não foi possível identificar uma definição formal e consolidada em documentos oficiais internacionais, sendo este conceito predominantemente desenvolvido em contextos académicos.

Uma visão mais clássica, e de grande influência na literatura portuguesa, é apresentada por Carrilho, que entende a segurança pessoal como "o conjunto de medidas ativas e passivas destinadas a salvaguardar a integridade física de uma pessoa na sua vida oficial e/ou particular, levadas a efeito por pessoal especialmente preparado e vocacionado, em estreita colaboração com o seu protegido" (Carrilho, 2007, pág. 619). Esta perspetiva centra o conceito na salvaguarda da integridade física, assumindo a proteção como binária (ativa e passiva) e colocando o foco principal na pessoa do protegido e na relação de proximidade com a equipa operacional de proteção. Porém, revela-se redutora à luz daquilo que são as exigências

contemporâneas, não considerando a natureza multidisciplinar da atividade e a articulação com outros atores atuais pertencentes à esfera da segurança pessoal.

Neste sentido, Lamano (2000) introduz uma conceção mais abrangente e ajustada à complexidade atual da atividade. Para este autor, a segurança pessoal não se limita à proteção física, implicando também a criação de "um ambiente seguro da entidade na sua integridade, no seu carácter, na sua reputação e que contribua para a melhoria de qualidade de vida" (p. 91). Este entendimento reconhece que a atuação do protetor ultrapassa a dimensão corporal e englobando também aspetos simbólicos, emocionais, protocolares e relacionais, integrando uma visão mais abrangente da segurança. Este conceito, inovador na sua época, aproxima-se da prática atual das unidades de segurança pessoal, para as quais a proteção da reputação e do estatuto protocolar, se incluem como parte essencial da missão.

Por fim, Magalhães (2018) sintetiza a segurança pessoal como uma atividade simultaneamente focalizada e multidimensional. Trata-se de uma missão focalizada porque incide sobre um conjunto restrito de beneficiários, delimitado pela lei e por critérios administrativos específicos. Esta focalização, porém, não corresponde a qualquer elitismo, refletindo apenas a aplicação de parâmetros jurídicos e operacionais rigorosos que identificam quem necessita de proteção especializada. Todavia, num plano mais amplo, a segurança pessoal articula-se com o dispositivo de Segurança Interna, partilhando informação, cooperando com estruturas de policiamento em grandes eventos e articulando-se com outras entidades quando o contexto o exige.

Destarte, para efeitos desta dissertação, entendemos por segurança pessoal a atividade policial, integrada e multidisciplinar, de carácter temporário ou contínuo, orientada a proteger, no plano preventivo, reativo e repressivo, um conjunto restrito de entidades. Esta atividade visa salvaguardar não apenas a integridade física do protegido, mas também a sua reputação, o seu estatuto protocolar e as condições indispensáveis ao exercício pleno das suas funções, contribuindo simultaneamente para a qualidade de vida e para a preservação da estabilidade institucional do Estado, numa relação baseada na confiança recíproca entre protetores e protegidos.

I.2 Evolução e Enquadramento Histórico

I.2.1 Violência Política e Proteção de Dignitários em Portugal

De forma a melhor compreender a evolução e todo o enquadramento histórico da segurança pessoal em Portugal, exige-se que se comece pelo reconhecimento de que o país foi,

durante largas fases da sua história, marcado por episódios de violência política que colocaram os titulares de cargos públicos em risco real. Como refere Magalhães (2018), o sentimento de segurança que Portugal hoje projeta é muito contrastante com o passado onde o país registou o assassinato de um Rei, de um Presidente e de um Primeiro-ministro, bem como diversos outros atentados de impacto variável que deixaram marcas profundas na memória coletiva nacional.

Também no contexto europeu era notória uma certa instabilidade, registando-se no final do século XIX que diversos movimentos anarquistas proliferavam e defendiam a ação direta como meio de transformação social, recorrendo frequentemente a atentados contra altos membros do Governo. Como refere Henriques et al (2008), estes grupos viam na ação violenta "o principal método de luta, visando destruir a sociedade capitalista e o Estado" (p. 65), o que reflete perceção de insegurança da época.

Um dos episódios mais marcantes e que há registo em território nacional é o regicídio de 1908, no qual D. Carlos I e o príncipe herdeiro D. Luís Filipe foram mortos por Manuel Buiça e Alfredo Costa. Para Samara & Tavares (2008), "de repente, a Europa descobria que as suas cabeças coroadas podiam ser assassinadas em plena luz do dia e que os acontecimentos andavam mais depressa do que era possível apanhá-los, talvez fosse a isto que chamavam tempos modernos" (p.134). A constante ameaça ao monarca era amplamente reconhecida, sobretudo após o decreto régio que conferiu a João Franco amplos poderes repressivos. O próprio D. Carlos terá afirmado, no momento da assinatura: "assino a minha sentença de morte, mas os senhores assim o quiseram" (Ramos, 2006, p. 313).

Este mesmo episódio acaba por levantar algumas questões que permanecem relevantes para a doutrina de segurança pessoal, como o motivo pelo qual, face ao clima de exaltação que se vivia em Lisboa, foi escolhida uma viatura aberta (landau) ao invés de uma carruagem fechada ou um automóvel, isto para além do itinerário escolhido, junto a locais onde era conhecida a concentração de grupos violentos contestatários da monarquia, decisões estas que nos dias de hoje seriam consideradas inadequadas após uma análise de risco.

Com o surgimento da Primeira República, o clima securitário manteve-se muito instável. Em dezembro de 1918, o Presidente Sidónio Pais foi assassinado na estação do Rossio. Como relata Telo, "o Presidente chegou à estação dos comboios, mesmo alertado para os perigos que corria, não hesita e decidiu viajar. Na estação José Júlio da Costa empurrou dois polícias e disparou 2 tiros no peito do Presidente" (Telo, 2011, p.65). Tal atentado ocorreu dias após uma tentativa falhada, quando um jovem lhe apontou uma pistola ao peito que não disparou. O Presidente ignorou igualmente avisos sobre atentados planeados durante a

deslocação ao Porto, demonstrando uma subestimação clara das ameaças, revelando assim uma atitude semelhante à atribuída, anos antes, a D. Carlos I.

Em 1921, a chamada "Noite Sangrenta" vitimaria o Primeiro-Ministro António Granjo, brutalmente assassinado a tiro e à baioneta no interior do quartel da Armada, num dos episódios mais violentos da Primeira República. Esta violência política parecia persistir mesmo durante o Estado Novo, quando Oliveira Salazar foi alvo de um atentado à bomba a 4 de julho de 1937. Como narra Madeira (2013), aquando da passagem da sua viatura pela Avenida Barbosa du Bocage, "uma enorme explosão atroa os ares esventrando a rua" (p.23), e abrindo uma cratera que evidenciava a intenção clara de assassinar o Presidente do Conselho. Apesar da violência da explosão, Salazar saiu ileso.

Durante o Estado Novo destacam-se outras ações terroristas, não especificamente direcionadas a altas entidades, mas com forte mediatismo e abanando as estruturas e convicção de invulnerabilidade por parte do regime do Estado Novo. São exemplo disso o sequestro do paquete Santa Maria de 21 para 22 de janeiro de 1961, por um grupo de 23 exilados políticos portugueses e espanhóis integrantes do designado Diretório Revolucionário Ibérico de Libertação que então faziam oposição política aos governos de António de Oliveira Salazar e de Francisco Franco, sob o comando do capitão Henrique Galvão e de Jorge de Soutomayor foi um ato que gozou de grande atenção mediática internacional. O Santa Maria realizava um roteiro turístico em janeiro de 1961, com 612 passageiros (principalmente americanos, portugueses e espanhóis), partindo de Lisboa para Miami. Durante a ação foi morto o oficial de bordo João Costa. A embarcação acabou por fundear no porto do Recife, no Brasil, em 2 de fevereiro seguinte, onde os sequestradores receberam asilo político, garantindo que não seriam extraditados para Portugal ou Espanha, evitando assim as ditaduras de Salazar e Franco. Também a 26 de outubro de 1970, o grupo terrorista de extrema-esquerda Ação Revolucionária Armada realizou a sua primeira ação, sabotando o navio Cunene no porto de Lisboa, o qual, se preparava para partir com material militar para África. O navio sofreu duas grandes explosões, ficando imobilizado para reparações durante vários dias, o que retardou a missão militar. Este mesmo grupo terrorista, em janeiro de 1972, destruiu material de guerra sofisticado vindo da França que seguia num navio para a guerra colonial, executando também em julho, uma outra tentativa malsucedida de sabotagem a noutro navio.

Após o Revolução do 25 de abril de 1974, e a instauração de um regime democrático, Portugal não ficou imune à vaga europeia de ações terroristas. A partir do final dos anos 1970 registaram-se no país atentados de grande impacto político, muitos deles associados ao

terrorismo transnacional. Entre esses episódios destaca-se o ataque de 13 de novembro de 1979 contra o embaixador de Israel, Ephraim Eldar, perpetrado por um comando armado da Organização de Libertação da Palestina. Embora o diplomata tenha sobrevivido, o guarda responsável pela sua proteção, Ildefonso Pereira, morreu no local, tendo "cumprido o seu dever ao protegê-lo" (Magalhães, 2018, p.43).

Um outro momento significativo ocorreu a 4 de dezembro de 1980, quando o ministro Adelino Amaro da Costa e o Primeiro-Ministro Sá Carneiro morreram na queda do avião Cessna, em Camarate. Após este evento fatídico, abriram-se múltiplas comissões parlamentares, sendo que a última considerou o episódio também como resultante de um atentado político. A estes episódios acrescenta-se também o atentado cometido em 12 de maio de 1982, quando, no Santuário de Fátima, o padre espanhol Juan Maria Fernández Krohn tentou assassinar o Papa João Paulo II com uma baioneta Mauser. A pronta intervenção dos polícias de segurança pessoal impediu que o ataque tivesse sucesso, reforçando, num momento transmitido em direto para todo o mundo, a sua importância para com a segurança de altas entidades (Magalhães, 2018).

Logo no ano seguinte, em 10 de abril de 1983, ocorreu o assassinato de Issam Sartawi, representante da Organização da Libertação da Palestina, durante o Congresso da Internacional Socialista, em Albufeira. Sartawi recusara as medidas de proteção disponibilizadas pelo Estado português, ao contrário de outros participantes que dispunham de equipas dedicadas, o que aumentou significativamente a sua vulnerabilidade. Foi abatido por terroristas ligados à organização palestiniana Abu Nidal, demonstrando mais uma vez que o facto de negligenciar o apoio dos elementos de segurança pessoal poderá ter consequências fatídicas, sobretudo tudo quando a análise de risco torna evidente essa possibilidade.

De destacar que a 27 de julho de 1983, um comando do Exército Revolucionário Arménio composto por cinco terroristas assalta a Embaixada da Turquia em Lisboa, tendo este ataque culminado com a morte dos cinco assaltantes, um polícia português e a mulher de um diplomata turco. Esta foi a primeira vez que à data o recém criado Grupo de Operações Especiais da PSP interveio numa situação real.

O último grande atentado desta sequência ocorre a 15 de fevereiro de 1986, quando Gaspar Castelo Branco, antigo Diretor-Geral dos Serviços Prisionais, é assassinado por elementos das Forças Populares 25 de Abril. Como é descrito por Magalhães (2018), o dirigente dispensava constantemente a sua equipa de segurança pessoal, o que aconteceu também naquele dia, aumentando o risco a que estava exposto.

Para Torres (2018, p.18), estes atentados permanecem "distantes na memória coletiva", mas não podem conduzir a um falso sentimento de imunidade nacional, uma vez que as sociedades contemporâneas, que Giddens (2000, p.29) designa de "cosmopolitas globais", são caracterizadas por ameaças difusas, imprevisíveis e frequentemente dirigidas contra alvos vulneráveis. Embora Portugal tenha estado imune a ataques deste tipo nas últimas décadas, a ideia de que o país "goza da garantia quase divina" de que nada ocorrerá, como ironiza Torres (2018, p.18), não passa de uma ilusão muito perigosa e inconsciente.

I.2.2 Consolidação e Criação do Corpo de Segurança Pessoal

Num contexto marcado por uma intensificação da ameaça terrorista em território nacional, tornou-se evidente a necessidade de dispor de estruturas policiais especializadas e de serviços de segurança capazes de antecipar, prevenir e enfrentar formas de criminalidade particularmente graves e complexas. Todavia, segundo Santos (2020), nos anos imediatamente subsequentes à Revolução de Abril de 1974, as prioridades dos primeiros Governos Constitucionais centraram-se predominantemente em questões de natureza económica e social, designadamente no combate ao desemprego, à inflação e ao défice estrutural de infraestruturas, num ambiente político caracterizado por elevada instabilidade. Só a partir de 1982, com a primeira revisão da Constituição da República Portuguesa (CRP), se procedeu a uma clarificação substantiva das funções e limites de atuação das forças armadas e das forças de segurança, criando-se, desse modo, as condições jurídico-institucionais necessárias à consolidação e organização de um verdadeiro sistema de segurança interna em Portugal (Fernandes 2014).

Introduz-se assim a expressão "Segurança Interna" na revisão constitucional de 1982, no artigo 272.º da CRP, enquanto função da Polícia. O debate político e social em torno da tensão entre liberdade e segurança dos cidadãos assumiu particular relevância no processo de consolidação da democracia portuguesa. Esta discussão revelou-se determinante para a aceleração da criação de instrumentos estruturantes do sistema de segurança interna, visando garantir a proteção da ordem constitucional (Santos, 2020).

No âmbito da segurança pessoal, tornou-se necessária a definição clara da responsabilidade da PSP na proteção dos órgãos de soberania. Essa clarificação foi concretizada com a revisão do primeiro Estatuto da PSP[1], que lhe atribuiu expressamente a missão de garantir a segurança pessoal dos membros dos órgãos de soberania, de altas entidades

[1] Cfr. Decreto-Lei n.º 151/85, de 9 de maio

nacionais ou estrangeiras e de cidadãos sujeitos a ameaça relevante, remetendo a regulamentação das condições e meios para despacho do Ministro da Administração Interna.

Perante a ausência inicial de normas de execução, o Comando-Geral da PSP (atual Direção Nacional da PSP), operacionalizou esta missão através da, na época, Divisão de Segurança do Comando Distrital de Lisboa, restringindo-a a polícias com formação especializada em segurança pessoal.

As especificidades da atividade de segurança pessoal evidenciaram a necessidade de uma estrutura autónoma, distinta do serviço policial convencional. Essa opção consolidou-se em 1994, no âmbito da reestruturação da PSP, com a aprovação da nova Lei Orgânica[2], que consagrou a segurança pessoal como competência exclusiva da PSP e instituiu formalmente o Corpo de Segurança Pessoal (CSP) (Santos, 2020).

Com grande reforma orgânica da PSP de 1999[3], ficou consagrado a designação de Direção Nacional da PSP e, de forma inédita, a chefia passou a ser exercida por um Oficial formado na Escola Superior de Polícia (atual ISCPSI), em substituição de um Oficial do Exército. Desta forma, constitui-se também um novo marco na afirmação da segurança pessoal, ao configurar o CSP como unidade autónoma, colocada na dependência direta do Diretor Nacional da PSP (Santos, 2020). Este processo de autonomização foi acompanhado pela consolidação de símbolos identitários próprios, como a criação de brasão de armas e, posteriormente, de boina e distintivo específicos, elementos que contribuíram para a afirmação da especialidade enquanto estrutura específica, dotada de identidade institucional própria.

Nos tempos que se seguiram, houve, segundo Farinha (2007), a necessidade de estabelecer maior coordenação e complementaridade perante as valências especiais da PSP, e conforme a última reforma à Lei Orgânica da PSP[4] (LOPSP), cria-se a Unidade Especial de Polícia (UEP), integrando-se as competências especiais numa única estrutura orgânica. A segurança pessoal passa a integrar uma das cinco valências da UEP, assumida pela subunidade do CSP. De notar também que, em matéria de competências exclusivas do CSP, a LOPSP apenas acrescenta a vertente da proteção policial de testemunhas às anteriores valências já supramencionadas.

Segundo Santos (2020), ao longo do seu processo de consolidação, a atividade de segurança pessoal necessitou de acompanhar as transformações do contexto securitário

[2] Decreto-Lei n.º 321/94, de 29 de dezembro
[3] Lei n.º 5/99, de 27 de janeiro
[4] Lei n.º 53/2007, de 31 de agosto

nacional e internacional, adaptando-se às melhores práticas observadas no próprio país e no estrangeiro. O seu raio de ação não se circunscreve ao território nacional, uma vez que a proteção permanente de determinadas entidades implica igualmente o acompanhamento policial além-fronteiras, incluindo a participação em missões internacionais, exercícios conjuntos e ações de formação no quadro das relações bilaterais. Importa ainda salientar que, desde a constituição do CSP, não se regista qualquer fatalidade no cumprimento da missão, facto que reflete o rigor, o profissionalismo e a maturidade operacional desta especialidade.

I. 3. Enquadramento Jurídico e Institucional do Corpo de Segurança Pessoal

No âmbito da presente investigação, revela-se importante referir que excluímos expressamente os serviços de proteção de pessoas prestados por particulares ou por empresas de segurança privada. Em Portugal, esta vertente encontra-se enquadrada no regime jurídico da segurança privada, sendo designada pelo legislador como "proteção pessoal". A Lei da Segurança Privada[5] define esta atividade no artigo 2.º, alínea o), como "a atividade de segurança privada de acompanhamento de pessoas, efetuada por vigilante de proteção e acompanhamento pessoal, para sua defesa e proteção".

Apesar do legislador não ter procedido à consagração de uma definição legal de "segurança pessoal", mantendo a expressão como conceito jurídico indeterminado, não se coloca qualquer risco de confusão entre ambos os institutos. Tal distinção resulta, desde logo, da diversa natureza jurídica das atividades: enquanto a proteção pessoal se insere na vertente do domínio do direito privado, a segurança pessoal constitui uma função pública, integrada nas atribuições do Estado. É precisamente por essa razão que, no ordenamento jurídico português, os conceitos de proteção pessoal e de segurança pessoal são realidades juridicamente distintas (Santos, 2020).

Para além da exclusão da segurança privada, importa igualmente clarificar que a segurança pessoal não se confunde com a proteção policial, ainda que ambas tutelem bens jurídicos pessoais idênticos. A distinção entre estes dois conceitos é fundamental para a correta delimitação do objeto de estudo. Desde logo, a segurança pessoal configura uma atividade de Segurança Interna, cuja aplicação compete ao poder executivo, inserindo-se na esfera da atuação preventiva e administrativa do Estado. Em contraste, a Proteção Policial insere-se no domínio da função jurisdicional, sendo atribuída exclusivamente por determinação da autoridade judiciária competente.

[5] Lei n.º 34/2013, de 16 de maio

Deste modo, o presente trabalho circunscreve-se exclusivamente ao estudo da segurança pessoal enquanto função pública, exercida por trabalhadores do Estado, integrada na organização e nas atribuições da Segurança Interna. Ficam, por conseguinte, fora do seu âmbito quer a proteção pessoal prestada por entidades privadas, quer a proteção policial determinada no contexto de processos penais, por se tratar de institutos distintos quanto à natureza, fundamento jurídico e entidade competente para a sua atribuição.

I.3.1. A Segurança Pessoal como Atribuição Legal

A segurança pessoal encontra-se expressamente consagrada como atribuição legal da PSP. Nos termos do artigo 3.º, n.º 3, alínea c), da LOPSP, compete à PSP "garantir a segurança pessoal dos membros dos órgãos de soberania e de altas entidades nacionais ou estrangeiras, bem como de outros cidadãos, quando sujeitos a situação de ameaça relevante".

A prossecução desta atribuição insere-se plenamente no domínio da Segurança Interna exercida pela PSP, assumindo particular relevância a Lei de Segurança Interna[6] (LSI). Com efeito, sendo a Segurança Interna uma das funções constitucionalmente atribuídas à Polícia (artigo 272.º, n.º 1, da CRP), a segurança pessoal acaba por também partilhar os mesmos fins e princípios, designadamente a garantia da ordem e tranquilidade públicas, a proteção de pessoas, a prevenção da criminalidade e a garantia do normal funcionamento das instituições democráticas (Santos, 2020).

A segurança pessoal surge, assim, integrada no elenco das atribuições adicionais da PSP, previstas no artigo 3.º da LOPSP. Segundo Santos (2020), esta classificação como atribuição adicional decorre, da própria construção normativa do preceito, que distingue entre atribuições gerais, partilhadas com outras Forças de Segurança, e atribuições especificamente cometidas à PSP. Evita-se também, deliberadamente, a qualificação destas atribuições como exclusivas, uma vez que, na reforma da orgânica da PSP, o legislador optou por suprimir a expressão "atribuição exclusiva", incluindo no domínio da segurança pessoal.

I.3.2. Competência Institucional e Especialização Funcional

Ainda nos termos do artigo 3.º, n.º 3, alínea c), da LOPSP, é à PSP que cabe garantir a segurança pessoal dos destinatários legalmente previstos. Para assegurar a prossecução desta atribuição, a PSP dispõe de órgãos e serviços especializados, dotados das competências necessárias ao desempenho da missão.

[6] Lei n.º 53/2008, de 29 de agosto

Neste contexto, a segurança pessoal constitui uma competência cometida à UEP, conforme resulta do artigo 40.º da LOPSP. Esta unidade compreende cinco subunidades operacionais, entre as quais se encontra o CSP, sendo este o serviço especificamente encarregado da execução da missão de segurança pessoal (artigo 44.º da LOPSP).

Desta forma concluímos que o CSP apenas pode desenvolver as tarefas que lhe são legalmente cometidas, na estrita prossecução dos respetivos fins institucionais. A atuação do CSP encontra-se, assim, juridicamente delimitada, sendo exercida no quadro das competências atribuídas pela lei e subordinada aos princípios da legalidade, da proporcionalidade e da necessidade.

I.3.3. Destinatários da Segurança Pessoal

Nos termos da LOPSP, a segurança pessoal abrange três grandes categorias de beneficiários: os órgãos de soberania, as altas entidades e outros cidadãos sujeitos a ameaça. Relativamente aos órgãos de soberania, a CRP estabelece no seu artigo 110.º que estes são o Presidente da República, a Assembleia da República, o Governo e os Tribunais.

Santos (2020) evidencia aqui uma lacuna dado que a LOPSP, não densifica quais os beneficiários concretos das medidas de segurança pessoal no caso dos órgãos de soberania de natureza colegial. A Assembleia da República, por exemplo, é composta por todos os deputados eleitos, enquanto o Governo integra Ministros, Secretários de Estado e, eventualmente, Subsecretários de Estado. Também relativamente aos Tribunais, não se esclarece se as medidas recaem apenas sobre representantes dos tribunais superiores ou sobre qualquer juiz. Esta densificação é, em grande medida, efetuada no âmbito das opções do executivo em matéria de Segurança Interna.

Para além dos órgãos de soberania e das altas entidades, a segurança pessoal pode ainda ser atribuída a "outros cidadãos sujeitos a ameaça". Entende-se que aqui podem incluir-se todas as pessoas, relativamente às quais exista um cenário de ameaça que justifique a adoção de medidas de segurança pessoal, desde que esteja em causa um interesse manifestamente público, nos termos do artigo 266.º, n.º 1, da CRP. Desta forma, podem integrar-se neste grupo dirigentes políticos, representantes religiosos ou da sociedade civil, atletas e respetivas comitivas, adidos e comitivas militares, entre outros. Excluem-se, contudo, as testemunhas em processo penal, às quais se aplicam, como já fora esclarecido, a medidas próprias de proteção policial.

Em síntese, os destinatários da segurança pessoal serão, de um modo geral, os titulares dos órgãos de soberania previstos constitucionalmente, as altas entidades legalmente

qualificadas e outros cidadãos relativamente aos quais exista uma ameaça especial cuja prevenção corresponda a um interesse público relevante.

I.3.4. Modalidades de Atribuição da Segurança Pessoal

Em determinados casos, a atribuição de segurança pessoal encontra-se expressamente prevista na lei. É o que sucede relativamente ao Presidente da República , enquanto órgão de soberania, onde se integra o Serviço de Segurança, que constitui a estrutura especialmente encarregada da sua proteção e segurança pessoal. Trata-se de um dos seis Serviços de apoio direto ao Presidente da República, com plena autonomia e direção operacional nos processos (atribuições e missões) de Segurança, é dirigido por um chefe de Serviço, que é o Oficial de Segurança do Presidente da República, e "integrado por um destacamento da Divisão de Segurança da Polícia de Segurança Pública, um destacamento da Guarda Nacional Republicana e uma esquadra da Polícia de Segurança Pública"[7]. Ao CSP cabem, pois, as missões de proteção e segurança pessoal do Presidente da República e respetivos familiares (quando aplicável)[8].

De igual modo, o regime orgânico do Gabinete do Primeiro-Ministro prevê um Serviço de Segurança, assegurado, em regime de exclusividade, por polícias do CSP[9].

Para todos os demais beneficiários, o instrumento que determina a aplicação de medidas de segurança pessoal é o Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança (PCCCOFSS), aprovado pela Deliberação n.º 140/2010, de 25 de março, do Conselho de Ministros. Este documento, classificado no grau de segurança "CONFIDENCIAL", define as medidas e operações concertadas no âmbito da Segurança Interna, incluindo a proteção de altas entidades e de cidadãos sujeitos a ameaça.

De acordo com o referido Plano, a aplicação das medidas de segurança pessoal depende essencialmente do grau de ameaça avaliado *a priori*, da categoria da entidade e da natureza da visita, distinguindo-se entre segurança permanente, temporária ou apenas associada a visitas oficiais (Ferreira de Oliveira, 2015; Magalhães, 2018).

A atribuição de segurança pessoal depende, assim, de um indicador de risco. Para esse efeito, foi adotada a escala comum de avaliação da ameaça para personalidades oficiais em visita à União Europeia, criada pelo Conselho Europeu e utilizada no intercâmbio de

[7] cfr. Lei n.º 7/96, de 29 de fevereiro, art.º 10.º.
[8] cfr. Programa de Segurança da Presidência da República, aprovado em 23 de junho de 2021 pelo Conselho Administrativo da Presidência da República. Classificado no grau de segurança "CONFIDENCIAL", constitui o documento estruturante que tipifica o conjunto de medidas e procedimentos que promovem e asseguram a prevenção, controlo, vigilância, proteção, segurança e defesa dos ativos críticos da Presidência da República.
[9] cfr. Decreto-Lei n.º 12/2012, de 20 de janeiro, art.º 7.º

intelligence entre os serviços de informações e as Forças de Segurança (Carrilho, 2007). Este será um tópico a aprofundar no capítulo II desta investigação, sendo que se adianta que a competência para avaliar o grau de ameaça é externa à PSP, cabendo ao Sistema de Informações de Segurança (SIS) essa avaliação prévia, a qual é posteriormente comunicada à PSP para efeitos de aplicação das respetivas medidas.

I.3.5. Orgânica do Corpo de Segurança Pessoal

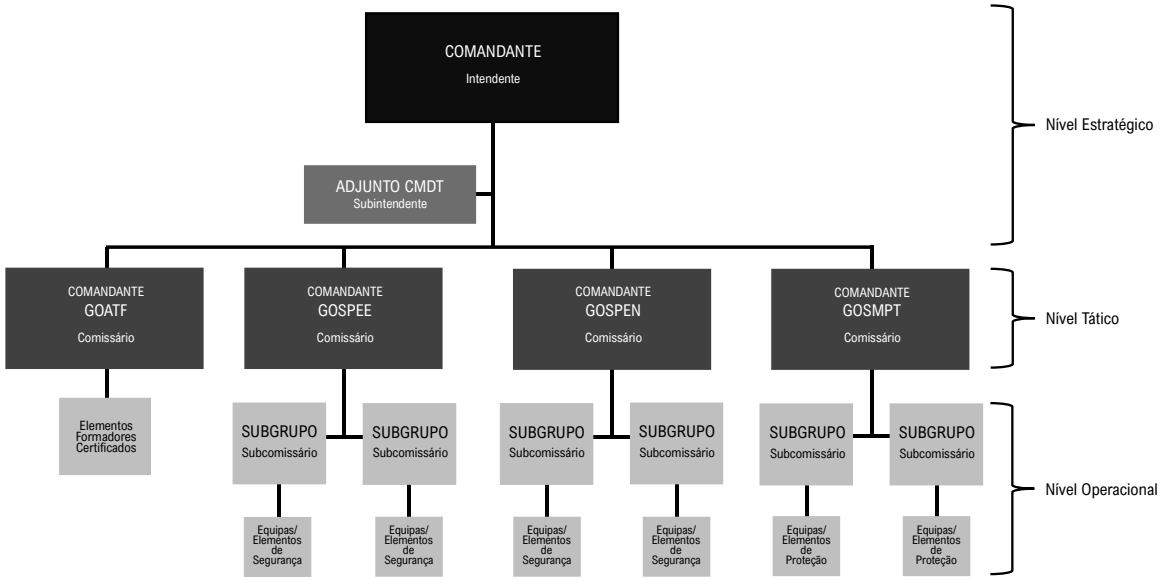
Relativamente à organização interna do CSP[10], este estrutura-se segundo um modelo funcional que visa responder às diferentes tipologias de missões que lhe são atribuídas. No plano da direção, o CSP integra um Comando, composto pelo comandante e pelo adjunto do comandante, aos quais compete a coordenação global da atividade operacional e a supervisão das equipas de segurança pessoal.

No plano operacional, a atividade do CSP encontra-se repartida por grupos especializados, organizados em função do tipo de entidades a proteger e da natureza das missões desempenhadas. As equipas de segurança pessoal distribuem-se por três grupos operacionais distintos: o Grupo Operacional de Segurança pessoal de Entidades Nacionais (GOSPEN), o Grupo Operacional de Segurança Pessoal de Entidades Estrangeiras (GOSPEE) e o Grupo Operacional de Segurança Pessoal a Magistrados e Testemunhas (GOSPMT). Complementarmente, existe ainda um Grupo Operacional de Apoio Técnico e de Formação (GOATF), responsável pelas componentes técnicas, formativas e de especialização necessárias ao desempenho das missões da subunidade.

[10] Cfr. Despacho 3/GDN/2026 - Orgânica da Unidade Especial de Polícia

Figura 1

Organização Hierárquica dos Serviços do CSP



Nota: Adaptado de Abreu (2015), com base Orgânica da UEP - Anexo 2 da O. S. N.º 25 de 5 de fevereiro de 2026)

O GOSPEN tem por missão assegurar a segurança pessoal de entidades nacionais, com exceção do Presidente da República e do Primeiro-Ministro, cuja proteção e segurança pessoal é assegurada, respetivamente pelo Grupo Operacional de Segurança Pessoal ao Presidente da República (GOSPPR) e pelo Grupo Operacional de Segurança Pessoal ao Primeiro-ministro (GOSPM). No que concerne às entidades judiciais, o GOSPEN assume a proteção dos presidentes dos tribunais superiores, diferenciando-se assim do âmbito de atuação do GOSPMT.

O GOSPEE é responsável pela segurança pessoal de entidades estrangeiras em território nacional, quer se encontrem em visitas de Estado ou visitas oficiais, quer sejam residentes, como é o caso dos chefes de missão diplomática, designadamente embaixadores. Este grupo organiza-se operacionalmente através de uma Equipa de Turno, em serviço permanente, e de uma Reserva Operacional, em regime de prontidão, permitindo assegurar uma resposta contínua e adaptável às exigências do contexto internacional[11].

Por sua vez, o GOSPMT assume competências no domínio da proteção policial no âmbito do processo penal, bem como da segurança pessoal de magistrados. Ficam, contudo,

[11] cfr. Diretiva Interna CSP/UEP n.º 02/2012

excluídos da sua esfera de atuação os presidentes dos tribunais superiores, cuja proteção, como referido, compete ao GOSPEN.

I. 4. Modelos Internacionais de Proteção de Altas Entidades

Nos Estados democráticos consolidados, a segurança pessoal de altas entidades sujeitas a ameaça é, na maioria dos casos, assegurada por Forças de Segurança de natureza civil, integradas nos respetivos Sistemas de Segurança Interna. Apesar desta matriz comum, a forma como a segurança é organizada e operacionalizada varia refletindo as especificidades políticas, institucionais, sociais e culturais de cada Estado.

No que concerne ao contexto dos Estados Unidos da América, o modelo de proteção de altas entidades caracteriza-se por uma elevada especialização e pela coexistência de diferentes organismos com competências bem definidas. A estrutura protetiva assenta, essencialmente, em dois grandes fornecedores de segurança pessoal. Por um lado, o *Diplomatic Security*, integrado no *Department of State*, é responsável pela segurança pessoal do Secretário de Estado, tanto em território norte-americano como no estrangeiro, assumindo igualmente a proteção de dignitários estrangeiros em visita aos Estados Unidos, nomeadamente ministros, embaixadores e membros de casas reais, com exceção do soberano. Por outro lado, o *United States Secret Service*, integrado no *Department of Homeland Security*, assegura desde logo a proteção do Presidente em exercício de funções, do Vice-Presidente e dos ex-Presidentes, sendo ainda responsável pela segurança dos Chefes de Estado e de Governo estrangeiros durante visitas oficiais ao território norte-americano (Magalhães, 2018).

No contexto europeu, prevalece também a opção por estruturas policiais de natureza civilista para o desempenho da segurança pessoal de altas entidades. Os casos de Espanha e França constituem exemplos particularmente relevantes, não só pela proximidade geográfica, mas também porque apresentam modelos organizacionais muito semelhantes entre si.

Em Espanha, a segurança pessoal de altas entidades nacionais e estrangeiras é, em regra, assegurada pela *Policía Nacional*, através da *Unidad Central de Protección*, unidade integrada na *Comisaría General de Seguridad Ciudadana*, dependente da *Jefatura Central de Seguridad Ciudadana y Coordinación*. De acordo com a informação disponibilizada no site oficial da *Policía Nacional*, esta unidade é responsável pela proteção de altas individualidades do Estado, de personalidades estrangeiras em visita oficial, bem como de outras pessoas classificadas como de risco elevado, assumindo igualmente a segurança de edifícios e infraestruturas considerados de interesse estratégico para o Estado.

Todavia, importa clarificar que a segurança pessoal do Rei de Espanha e dos restantes membros da Família Real é da competência primária da *Guardia Civil,* uma força de segurança de natureza militar, configurada como Corpo Nacional de Gendarmaria, tutelada pelo Ministério da Defesa e Ministério do Interior. Sendo que a *Casa de S.M. el Rey* dispõe ainda de um *Servicio de Seguridad* próprio, responsável pela proteção direta da Chefia do Estado e do seu núcleo familiar, o qual funciona segundo um modelo integrado, incorporando efetivos *Cuerpo Nacional de Policía* e da *La Guardia Civil*.

A *Unidad Central de Protección* inclui duas brigadas especializadas: a *Brigada Central de Escoltas*, que garante a proteção integral de altas personalidades do Estado e de testemunhas protegidas, e a *Brigada Central de Protecciones Especiales*, que planeia e executa dispositivos de segurança para delegações estrangeiras em visita oficial, bem como para o transporte de obras de arte ou bens culturais de elevado valor. O dispositivo organiza-se em torno de um serviço central e de destacamentos permanentes junto da Presidência do Governo, do Congresso e do Senado.

Já em França, segundo a descrição disponível no site oficial do *Ministère de l'Intérieur* a missão de proteção de altas entidades é atribuída ao *Service de la Protection*, uma estrutura especializada da Polícia Nacional francesa. No seu seio, destaca-se o *Groupe de Sécurité de la Présidence de la République*, unidade mista composta por agentes da Polícia e da Gendarmaria, com responsabilidade exclusiva pela segurança pessoal do Presidente da República, tanto em território nacional como em deslocações oficiais ao estrangeiro, em articulação com os serviços de segurança dos países anfitriões. Paralelamente, o *Service de la Protection* inclui subdireções vocacionadas para a proteção de outros membros do Governo, de personalidades ameaçadas (nacionais ou estrangeiras) e de chefes de Estado em visita oficial. O dispositivo francês integra ainda destacamentos territoriais, nomeadamente na Córsega e em Estrasburgo, de forma a garantir uma cobertura descentralizada e adaptada às exigências institucionais e geográficas do país.

Por fim, e para além dos modelos norte-americano e europeus analisados, justifica-se ainda a referência ao caso israelita, não apenas pela sua singularidade no panorama internacional, mas sobretudo pelo facto de Israel ser reconhecido como um dos Estados mais avançados no domínio da proteção de altas entidades em contextos de ameaça permanente. Neste sentido, em Israel, a missão de assegurar a segurança pessoal das altas figuras do Estado é atribuída à *Israel Security Agency***,** pelo definido so site oficial, também conhecida como *Shabak* ou *Shin Bet*, o Serviço Nacional de Segurança Interna, operando sob a tutela direta do

Primeiro-Ministro. Entre as suas atribuições oficiais está a proteção do Presidente da República, do Primeiro-Ministro e de outras altas entidades governamentais, de representantes diplomáticos e de dignitários estrangeiros em visita ao país. A *Israel Security Agency* organiza esta missão através de uma divisão de proteção específica, que atua com autonomia operacional em todo o território nacional e colabora com outras entidades como a Polícia de Israel, as forças militares, e, quando necessário, com o *Mossad*, no caso de operações externas.

Capítulo II: A Inteligência Policial na Atividade Operacional

II. 1. Informações Policiais

II.1.1. Conceito e Estrutura das Informações Policiais na Polícia

No quadro da segurança interna, as informações policiais constituem a base de conhecimento a partir da qual se orienta a atividade quotidiana das forças e serviços de segurança, antecipando riscos, apoiando a decisão e fazendo a ligação, de forma sistemática, entre a observação do terreno e a definição das respostas operacionais e estratégicas. Neste sentido, antes de abordar a inteligência policial no seu sentido estrito, importa clarificar o que se entende por informações policiais.

A doutrina distingue claramente o conceito de informações policiais de outras formas de informação no domínio da Segurança Interna, sublinhando a sua natureza instrumental em relação à atividade das forças e serviços de segurança (Garcia, 2009). Na definição clássica de Medeiros (2001), as informações policiais são "um conjunto de atividades reguladas pelos princípios enformadores da segurança interna, alicerçados numa estrutura organizacional, que visam obter um conhecimento intrínseco à prossecução dos fins inerentes à missão policial" (p. 20). Nesta perspetiva, as informações policiais assumem um carácter eminentemente instrumental e interno, orientando-se para apoiar a decisão dos comandos e dos responsáveis operacionais, em articulação com as exigências legais de respeito pelos direitos, liberdades e garantias.

Vários autores convergem ainda na distinção entre notícias, informações e conhecimento, enquanto patamares sucessivos de tratamento da realidade empírica. As notícias são assim entendidas como "qualquer facto, documento ou material, cujo conhecimento se revele suscetível de ter interesse para as finalidades de atuação de um serviço de informações" (Shulsky, 1991, p. 189). Já Bispo (2004) define que

> as informações consistem na análise da informação no sentido da obtenção de conhecimento, constituem-se como patamar acima da informação, como o trabalho efetuado sobre os dados para lhes dar sentido no quadro dos propósitos a quem ele serve, seja o Estado, a Polícia ou um serviço. É uma compreensão da informação relacionada, organizada e contextualizada. (p.77)

Nesta linha, Garcia (2009) sintetiza que "as informações diferem das notícias na medida em que as primeiras são o resultado do processamento e tratamento das segundas" (p. 11),

reforçando a ideia de que nem todos os dados recolhidos se transformam em verdadeiro conhecimento útil para a decisão.

De notar que, embora existam organismos do Estado especificamente vocacionados para a pesquisa e tratamento de notícias e informações de segurança, designadamente o SIS, a atividade informativa não se esgota nesses serviços, já que a finalidade das informações varia em função da missão de cada instituição, mantendo-se, em todos os casos, como meio essencial para o cumprimento das respetivas atribuições. Nesta linha, Fernandes & Valente (2005) defendem que

> o conceito de informações, no âmbito da segurança interna, deve ser entendido numa dupla vertente: enquanto atividade destinada à produção de informações de segurança (desenvolvida exclusivamente pelos serviços de informações […]) e enquanto atividade instrumental, destinada a contribuir para a investigação criminal, segurança e ordem públicas. (p. 34–36)

No contexto da PSP, o processo de produção de informações encontra suporte numa estrutura orgânica específica, definida na Lei Orgânica da PSP, que integra, em particular, o Departamento de Informações Policiais (DIP) e o Departamento de Investigação Criminal (DIC).

No caso do DIP, este é composto por duas divisões: a Divisão de Análise e Cooperação (DACO) e a Divisão de Segurança e Gestão da Informação (DSGI)[12]. Segundo o Artigo 5º da Portaria n.º 383/2008, alterada pela Portaria n.º 379-B/2023, de 17 de novembro, cabe-lhe, entre outras competências, "proceder à recolha e processamento de notícias com interesse para a missão policial"; "proceder à análise e avaliação de riscos específicos, associados ao cumprimento das missões da PSP"; "centralizar, partilhar e gerir a nível nacional a informação policial, assegurando a ligação permanente com entidades externas nesse domínio" e "centralizar, gerir e partilhar a nível nacional as informações desportivas […]", assumindo-se como o eixo central da atividade de informações policiais e de segurança na instituição. Por sua vez, o DIC engloba a Divisão de Investigação Criminal e Cooperação Internacional (DICCI) e a Divisão de Polícia Técnica e Ciência Forense (DPTCF)[13], concentrando as vertentes processual e operacional da investigação criminal e integra, no seu seio, estruturas de análise criminal que trabalham informações especificamente orientadas para o apoio às

[12] Despacho n.º 19935/2008 de 28 de julho, artigo 1º, n.º 1, alínea d)
[13] Despacho n.º 19935/2008, Artigo 1º, n.º 1, alínea e), alterado e republicado pelo Despacho 6158/2017, de 13 de julho

investigações e ao processo penal (Garcia, 2009). Compete-lhe, em particular, "coordenar e gerir o fluxo de informações criminais e conexas, no âmbito da cooperação internacional, com todos os organismos, com especial enfoque para aqueles nos quais a PSP se encontra representada"[14].

Antes de prosseguir, importa clarificar também alguns conceitos no âmbito da recolha de informações que pode ser organizada de acordo com as fontes e os meios utilizados para a sua obtenção, sendo comum, na literatura sobre inteligência, identificar quatro técnicas principais de recolha de informação.

Estas técnicas são habitualmente designadas por acrónimos de origem norte-americana: *Human Intelligence* (HUMINT), relativa à inteligência obtida através de fontes humanas; *Signals Intelligence* (SIGINT), referente à inteligência resultante da interceção e análise de sinais ou comunicações; *Imagery Intelligence* (IMINT), associada à recolha e interpretação de imagens obtidas por diferentes meios tecnológicos; e *Open Sources Intelligence* (OSINT), que corresponde à inteligência produzida a partir de fontes abertas. De destacar também que Elias (2023) defende também que a vertente da *Technical Intelligence* (TECHINT), relativa à inteligência obtida por fontes técnicas, está, de forma progressiva, a substituir o HUMINT, o policiamento de proximidade e as parcerias estabelecidas entre a polícia e as comunidades. O mesmo confirma a sua importância ao afirmar que "Uma abordagem integrada entre a estratégia de policiamento de proximidade, o *Intelligence-Led Policing*, o TECHINT e o HUMINT pode revelar-se crucial para prevenir e combater o crime, manter uma relação sólida com as comunidades locais e melhorar a qualidade do serviço policial." (Elias, 2023, p.33).

Em conjunto, estas modalidades constituem diferentes processos de recolha e gestão de informação que, através da sua articulação, permitem transformar dados em conhecimento relevante para a análise e tomada de decisão.

II.1.2 Informações de Fontes Abertas e Fontes Reservadas

A sociedade em rede e a massificação das tecnologias de informação criaram um contexto em que a produção de informações policiais não pode ser dissociada das fontes abertas, em particular das redes sociais. A revolução ao nível das tecnologias de informação e inteligência artificial transformou profundamente as noções de tempo, espaço e território, generalizando o acesso e a circulação de informação e conhecimento em escala global (Ferreira, 2012).

[14] Despacho 6158/2017, de 13 de julho, artigo 12º, n.º 1, alínea d)

Neste sentido, Ferreira (2012) refere também que a internet assume-se como infraestrutura básica de comunicação, resultado de um percurso que vai da *Arpanet*[15] às atuais redes mundiais, permitindo fluxos de dados quase instantâneos de informação. Nas palavras de Moreira (2010) "desenvolvimento da internet tem permitido à tecnologia digital a transmissão automática de todo o tipo de mensagens, criando, desta forma, uma linguagem digital universal e as condições tecnológicas para uma comunicação cada vez mais global" (p.657). A nível policial, isto significa que uma parte relevante dos comportamentos, manifestações de conflito, tensões e até práticas criminais passa a ter expressão, direta ou indireta, neste espaço digital.

É neste cenário que ganham relevo as fontes abertas, entendidas segundo Ferreira (2012) como toda a informação de acesso público, produzida e difundida sem restrições especiais de segurança. Em termos de vantagens, destaca-se o baixo custo e o elevado grau de oportunidade, embora se saliente igualmente o risco de excesso informacional, de qualidade variável, que obriga a uma triagem e validação rigorosas.

Quando estas fontes são tratadas de forma sistemática no âmbito da atividade de informações, costuma falar-se em OSINT, definido por Júnior (2008) como uma forma de gestão do conhecimento assente na recolha legal de informação disponível em meios públicos, nomeadamente media tradicionais, bases de dados abertas e conteúdos online, seguida da sua seleção, análise e consequente produção do conhecimento.

As redes sociais constituem uma das expressões mais relevantes das fontes abertas em ambiente digital, concentrando volumes significativos de informação gerada voluntariamente pelos utilizadores e frequentemente acessível a um público indeterminado. Operacionaliza-se assim, através do ciclo de produção de informações policiais, pesquisa em fontes abertas, avaliação de fiabilidade e análise estruturada que segundo Medeiros (2001) "é precisamente a análise, nas informações criminais, onde se estabelece a principal diferença entre o processo de produção de informações na vertente policial e o processo tradicional[16] " (p.35).

Para além das fontes abertas, importa referir sinteticamente as chamadas informações reservadas. Enquanto as fontes abertas correspondem à informação de acesso público, "disponível de forma completamente livre e aberta" consultável por qualquer cidadão (Ferreira, 2012, p. 25), as informações reservadas resultam de bases de dados internas, procedimentos de

[15] Acrónimo de Advanced Research Projects Agency Network, foi criada em 1969 para fins militares e de ocupação da vanguarda tecnológica, foi estabelecida pelo Departamento de Defesa dos EUA, vindo mais tarde a dar origem à Internet.

[16] Por "processo tradicional" compreende-se todo o tratamento e elaboração de informações desenvolvido pelos Serviços de Informações (ex.: SIS).

investigação, sistemas de informação criminal ou canais de cooperação que estão protegidos por regimes de segredo de justiça, segredo de Estado ou proteção de dados pessoais.

A proteção de fontes reservadas encontra fundamento nos princípios estruturantes da segurança das matérias classificadas, consagrados no SEGNAC 1[17], designadamente no princípio da necessidade de conhecer, na credenciação do pessoal e na classificação da informação. Em especial, quanto aos graus de segurança a atribuir às matérias, definidos no subcapítulo 3.2, as designações surgem de forma decrescente de classificação como: "Muito Secreto", "Secreto", "Confidencial", "Reservado", sendo nos subcapítulos seguintes definidas as entidades competentes para atribuir estes graus, assim como os respetivos procedimentos. Estes mecanismos asseguram a compartimentação da informação sensível, limitando o seu acesso a indivíduos devidamente autorizados e garantindo, assim, a salvaguarda da identidade e integridade das fontes.

A principal diferença reside, assim, na forma de acesso e tratamento, enquanto as fontes abertas podem ser autonomamente recolhidas e analisadas pelos serviços policiais, desde que respeitados os direitos fundamentais, ao passo que o acesso a informações reservadas exige sempre um enquadramento formal e estatutário. Isso significa atuar no âmbito de competências legalmente atribuídas e sob direção da autoridade judiciária (Lei n.º 49/2008) quando esteja em causa investigação criminal, não podendo os órgãos de polícia criminal movimentar-se livremente em bases de dados de outras entidades ou em sistemas de informações de segurança (Fortes, 2020).

Esta particularidade torna também indispensável uma boa rede de contactos institucionais. A lei sublinha que as forças e serviços de segurança devem cooperar "através da comunicação de informações que, não interessando apenas à prossecução dos objetivos específicos de cada um deles, sejam necessárias à realização das finalidades de outros", sempre com respeito pelos regimes aplicáveis (Lei n.º 53/2008, art. 6.º, n.º 2). Na prática, o acesso a informações reservadas de outras forças ou serviços faz-se por vias formais de cooperação, pontos únicos de contacto, sistemas integrados de informação criminal, unidades de coordenação, e não por recolha direta e informal, ao contrário do que sucede com as fontes abertas (Pereira, 2013).

[17] O SEGNAC 1 (Instruções para a Segurança Nacional, Salvaguarda e Defesa das Matérias Classificadas) foi aprovado pela Resolução do Conselho de Ministros n.º 50/88, de 3 de dezembro, ao abrigo Lei de Segurança Interna, constituindo um instrumento normativo de natureza regulamentar que estabelece os princípios e regras aplicáveis à proteção de matérias classificadas no âmbito da Administração Pública.

II. 2. Inteligência Policial como Instrumento da Segurança Interna

II.2.1 Conceito de Inteligência e Ciclo de Produção

A discussão do conceito de inteligência começa pela própria designação a adotar. Não existe consenso, isto porque, por vezes, utiliza-se "informações" e, outras vezes "inteligência" (Araújo, 2019). Em Portugal, a doutrina continua a ser maioritariamente marcada pelo uso de "informações", mas parte da investigação académica, incluindo Elias (2022) e Clemente (2009) já utilizam em paralelo os dois termos para designar realidades próximas.

Neste trabalho adota-se "inteligência" ou "*intelligence*" para designar o produto informacional final, mantendo "informações" para referir à valência existente na PSP, referida no subcapítulo anterior, que se ocupa da produção desse produto, em conformidade com a terminologia institucional. Esta opção é apoiada por Fernandes (2014), que considera "inteligência" uma designação mais completa, por refletir a articulação entre dados, informação e conhecimento, sendo este último o recurso central das organizações contemporâneas.

Deste modo, segundo Fernandes (2014) os dados constituem o nível de abstração mais elementar, sendo registos qualitativos ou quantitativos, extraídos da observação, que descrevem atributos ou características de uma variável, mas que, isoladamente, pouco significam. Já Araújo (2019) destaca que, enquanto entidades descontextualizadas, estes dados não possuem, por si só, qualquer significado inteligível. Quando organizados num determinado contexto e em função de um objetivo, esses dados convertem-se em informação, elevando o nível de abstração e permitindo já reduzir incerteza e identificar padrões (Oyedokun et al., 2022). Por fim, a informação transforma-se em conhecimento, o qual assume uma posição central na atividade das organizações, na medida em que orienta decisões e estratégias (Bonilla, 2004).

De acordo com Elias (2022) a inteligência assume-se como um dos vetores fulcrais da atividade policial, na medida em que permite manter a ordem pública, garantir a segurança e promover a paz em sociedade. Neste sentido, a inteligência revela-se essencial para a prevenção da ocorrência de crimes, através da recolha de informações relevantes que podem ser apresentadas sob diferentes formas bem como notícias, factos e dados que, mediante processos de metodologia e sistematização, são transformados em informação.

Na perspetiva de Palmieri (2005), a inteligência resulta de um processo de análise e interpretação aplicado a dados provenientes de diversas fontes, sendo o produto final desse tratamento o próprio *output* de inteligência. Trata-se, assim, de uma atividade que mobiliza diferentes métodos de recolha e técnicas de análise, orientada para "responder a necessidades

específicas de consumidores específicos, onde podem intervir variados atores" (Fernandes, 2014, p. 97).

Na sua formulação clássica, este trabalho de produção de Inteligência divide-se em cinco fases, designando o ciclo de produção de inteligência. Sendo essas fases, o planeamento e direção, a pesquisa, o processamento, a análise/produção e a difusão (Fernandes, 2014; Goldman, 2006; Elias, 2022).

De forma objetiva, no planeamento definem-se as necessidades de informação materializadas em Elementos Essenciais de Informação (EEI), que dão origem a um plano de pesquisa indicando o quê, como, quem e quando pesquisar (Fernandes, 2014). A pesquisa contempla a recolha de informação de fontes humanas, técnicas, abertas ou classificadas, mas nesta fase o resultado continua a ser apenas dados e informação em bruto, que só se convertem em inteligência após o processamento e a análise (Lowenthal, 2009). Na fase de processamento executam-se operações mais técnicas e uma primeira avaliação da confiança das fontes e da verosimilhança dos conteúdos, confrontando-os com informação pré-existente e com o contexto (Fernandes, 2014). Segue-se a análise e produção, em que o analista integra dados de várias origens, identifica padrões e elabora hipóteses ou estimativas para responder às necessidades dos decisores (Mangio & Wilkinson, 2008). Esta etapa é especialmente sensível ao modelo mental do analista, moldado pela sua formação e experiência, o que influencia a seleção da informação relevante e a interpretação dos sinais disponíveis (Pherson & Heuer, 2010). Os resultados materializam-se depois em relatórios, briefings ou outros produtos informacionais, sujeitos a revisão quanto à clareza, objetividade e coerência. A difusão encerra o ciclo, traduzindo-se na transferência controlada desses produtos para os consumidores (Lowenthal, 2009). Para ser eficaz, requer escolhas prévias sobre o que difundir, a quem dirigir cada produto, com que urgência e nível de detalhe, e sob que regime de classificação, respeitando o princípio da necessidade de conhecer (Fernandes, 2014). No contexto policial esta etapa é decisiva para que a inteligência seja efetivamente incorporada no planeamento de operações, nas ordens de serviço e na configuração dos dispositivos no terreno.

Tradicionalmente, estas funções eram exercidas por serviços públicos de informações, mas Ferreira (2023) refere que, atualmente, também as entidades privadas produzem inteligência, muitas vezes em articulação com Forças e Serviços de Segurança. Em Portugal, a função de avaliação global de ameaças ao nível nacional cabe, em exclusivo, ao Sistema de Informações da República Portuguesa (SIRP), composto, designadamente, pelo SIS e pelo

Serviço de Informações Estratégicas de Defesa (SIED), nos termos da Lei n.º 4/2014, de 13 de agosto.

O SIED, previsto no art.º 20.º da LQSIRP, é um organismo público que depende diretamente do Primeiro-Ministro e tem por missão produzir informações que contribuam para a salvaguarda da independência e dos interesses nacionais e da segurança externa do Estado. Segundo Fernandes (2014), esta missão concretiza-se através da "produção de inteligência relativa a eventos de natureza política, social, económica ou de segurança ocorridos no estrangeiro" (pág. 88). Sendo que esta inteligência se traduz em relatórios focados em regiões geográficas de interesse estratégico para Portugal, designadamente onde existam interesses económicos relevantes ou dependência energética, e em análises de mais abrangente, como as que incidem sobre o acesso a recursos naturais, o terrorismo, a criminalidade organizada transnacional ou a proliferação de armas de destruição maciça (Fernandes, 2014).

Paralelamente, o SIS, regulado pelo art.º 21.º da LQSIRP, é também um organismo público juridicamente autónomo, sob dependência direta do Primeiro-Ministro, com autonomia administrativa e financeira, cuja missão se centra na produção de informações relevantes para a salvaguarda da Segurança Interna. Compete-lhe, em particular, como descreve Fernandes (2014), contribuir para "a prevenção da sabotagem, do terrorismo e da espionagem, através de atividades de contrainteligência" (pág. 90). No fundo, e como será abordado mais adiante, estas atividades de contrainteligência visam identificar e neutralizar ameaças e riscos à segurança colocados por organizações ou indivíduos que procurem conhecer, sabotar ou comprometer as operações do Estado, bem como prevenir atos suscetíveis de alterar ou destruir o Estado de direito constitucionalmente estabelecido (Fernandes, 2014).

II.2.2 Inteligência Policial

Nos termos da Lei Orgânica da PSP, Lei n.º 53/2007, de 31 de agosto, a prossecução das missões de garantir a ordem e tranquilidade públicas, prevenir a criminalidade e investigar ilícitos, assenta crescentemente no uso sistemático de inteligência, sob pena de a decisão policial se apoiar em perceções fragmentadas ou meramente reativas (Carvalho, 2009).

À luz do descrito na NEP n.º AUOOS/DIP/02/05, a inteligência policial pode ser entendida como o conjunto de estruturas e atividades orientadas para a produção e difusão de informação relevante sobre riscos que incidem sobre as missões e atividades policiais, tendo como finalidade reduzir a incerteza e a surpresa no processo de tomada de decisão, bem como reforçar a eficácia, a proatividade e a resiliência institucional da PSP.

Ratcliffe (2007) reforça a sua natureza processual, descrevendo um encadeamento de obtenção, análise, avaliação, produção e divulgação de conhecimentos que permitem detetar condutas criminosas e respetivos infratores, orientar o policiamento e suportar decisões mais informadas no combate ao crime e na garantia da segurança pública. Fernandes (2014) destaca a dimensão organizacional desta função, ao caracterizar a inteligência policial como um conjunto de unidades especializadas que trabalham de forma multidisciplinar para produzir informação e conhecimento relevantes para os decisores.

Enquanto resultado, a inteligência policial organiza-se, em termos gerais, em inteligência estratégica e operacional (Fernandes, 2014; Ratcliffe, 2007). A inteligência estratégica centra-se na "avaliação dos padrões de criminalidade visados, tendências da criminalidade, organizações criminosas para efeitos de planeamento, tomada de decisões e distribuição de recursos" (Carter, 1990, p. 165). Tem uma natureza prospetiva e proativa e não visa reagir ao criminoso individual, mas sim a apoiar a definição de medidas preventivas ou mitigadoras de tendências e fenómenos criminais, sendo utilizada sobretudo pelos altos quadros responsáveis pelo planeamento a médio-longo prazo (Fernandes, 2014; Ratcliffe, 2007). Para além do planeamento interno, pode ainda identificar oportunidades de alteração legislativa e contribuir para políticas públicas que reforcem a prevenção e neutralização de riscos e ameaças à segurança pública (Fernandes, 2014).

Abaixo deste nível situa-se a inteligência operacional, entendida por Goldman (2006) como a inteligência necessária ao planeamento e execução bem-sucedida de operações que visam incrementar a segurança e a tranquilidade públicas. Auxilia os comandantes de áreas geográficas delimitadas a planear ações de redução da criminalidade e afetação de meios policiais. Isto permite identificar os grupos existentes numa dada área, a sua localização, quais são mais suscetíveis de vitimização e quais são mais propensos à prática de crimes, de modo a priorizar recursos em situações ou zonas com maior impacto na redução da criminalidade (Ratcliffe, 2007). Segundo Fernandes (2014), esta vertente relaciona-se estreitamente com a investigação criminal, ao apoiar a "identificação dos elementos específicos das ações criminais" (p.103), nomeadamente na identificação e seleção de alvos, deteção e intervenção sobre criminosos específicos. Segundo McDowell (2009), permite conhecer também o *modus operandi*, capacidades, limitações, vulnerabilidades, intenções e redes de apoio e financiamento, sendo tanto mais eficaz quanto mais se apoiar no trabalho de base de patrulhamento e na recolha sistemática e contínua de dados sobre a atividade rotineira das unidades e sobre as reações da comunidade.

A inteligência policial torna-se, assim, um suporte transversal à decisão em todos os níveis, reforçando a capacidade da PSP para antecipar riscos, orientar o emprego de meios e ajustar a atuação no terreno.

Face à constante evolução das técnicas utilizadas pelos agentes do crime, Pereira (2013) e Fernandes (2014) evidenciam que o uso sistemático de inteligência permite uma atuação mais dirigida, baseada no conhecimento da génese espacial e temporal do crime e de condutas reiteradas, ajudando a concentrar esforços em indivíduos, grupos ou locais críticos. Segundo Fernandes (2014) "A inteligência policial deve ser vista como a atividade que reforça o potencial de colaboração entre as polícias e os serviços de inteligência, contribuindo de forma determinante para a garantia da segurança interna" (p.169). Nesta perspetiva, a inteligência policial deixa de ser um mero apoio à investigação e passa a constituir um elemento central de planeamento e de gestão de risco na atividade diária da PSP, incluindo contextos específicos como a proteção de altas entidades.

II.2.3 Estrutura da Inteligência Policial na Polícia

A Lei n.º 30/84, de 5 de setembro, alterada pela Lei Orgânica n.º 4/2014, de 13 de agosto, que aprova a Lei Quadro do SIRP, estabelece que os serviços de informações têm por finalidade "assegurar, no respeito da Constituição e da lei, a produção de informações necessárias à preservação da segurança interna e externa, bem como à independência e interesses nacionais e à unidade e integridade do Estado" (art.º 2.º, n.º 2). Neste enquadramento mais lato do sistema de informações, Corrêa (2018) sublinha que a PSP criou, no seio do DIP, uma estrutura especificamente vocacionada para a produção de informações policiais necessárias ao cumprimento da missão policial, designada Sistema de Inteligência Policial da PSP (SINTEL).

A NEP n.º AUOOS/DIP/02/05, atualiza e aprofunda o SINTEL, enquadrando a atividade de inteligência da PSP com as ameaças e riscos que incidem sobre a segurança, ordem e tranquilidade pública e com as exigências da sua missão. Desta forma, fixam-se os princípios gerais de organização e funcionamento do sistema e clarifica conceitos centrais de inteligência policial. Nos termos do seu art.º 4.º, al. a) e d), o SINTEL pode ser entendido como um sistema integrado que agrega as diversas estruturas orgânicas e recursos humanos responsáveis pelo desenvolvimento das atividades de inteligência policial, funcionando de acordo com os princípios que orientam a sua organização e o seu modo de funcionamento.

Em termos estruturais, o SINTEL distribui-se por três níveis. Ao nível estratégico, o DIP da Direção Nacional assume a função de Unidade Estratégica do SINTEL (UE/SINTEL).

Num segundo patamar, os Núcleos de Informações Policiais (NIP) dos Comandos Regionais, Distritais, Metropolitanos e da UEP constituem as Unidades Operacionais (UO/SINTEL). Por fim, nas Esquadras e Divisões, as Secções de Operações e Informações (SOI) desempenham o papel de Subunidades Operacionais (SO/SINTEL). A UE/SINTEL centra-se no controlo e orientação estratégica do sistema, enquanto UO/SINTEL e SO/SINTEL funcionam como interfaces da inteligência ao nível dos comandos e das subunidades.

Uma das funções nucleares da UE/SINTEL é a definição das Áreas de Interesse Permanente (AIP)[18], isto é, os domínios temáticos sobre os quais todas as estruturas do SINTEL devem desenvolver esforços sistemáticos de recolha e análise. Estas AIP concretizam-se em Necessidades Prioritárias de Inteligência (NPI), que exprimem as necessidades mais relevantes para o planeamento e para a condução das atividades de inteligência. De forma articulada, o sistema procura assegurar a cooperação entre estruturas, responder a necessidades de inteligência sobre riscos que possam afetar as missões ou a imagem institucional da PSP e garantir mecanismos de intercâmbio de informação entre unidades policiais e Direção Nacional, com especial incidência nas AIP.

No plano operacional, compete às UO/SINTEL propor o planeamento operacional em função das necessidades de inteligência da unidade e das NPI, supervisionar e coordenar o trabalho das SO/SINTEL, apoiar essas subunidades na satisfação das suas necessidades informacionais e produzir produtos de inteligência compatíveis com os objetivos definidos na NEP n.º AUOOS/DIP/02/05. As SO/SINTEL são responsáveis por desenvolver as atividades de recolha, tratamento e produção de inteligência ao nível da subunidade e por difundir para a respetiva UO/SINTEL informação que possa interessar a outras UO/SINTEL, à UE/SINTEL, a outros serviços da PSP ou a outras forças e serviços de segurança.

Para garantir que a inteligência produzida circula de forma segura, rápida e tecnicamente adequada, a NEP cria o Canal Técnico de inteligência policial (CTINTEL). Este canal, paralelo à cadeia hierárquica, assegura o fluxo de informação e inteligência entre UE/SINTEL e UO/SINTEL, entre UO/SINTEL e SO/SINTEL e entre diferentes UO/SINTEL, podendo ser ativado por qualquer dos seus membros, sem obediência a escalões intermédios, mantendo-se a UE/SINTEL responsável pela supervisão e controlo do seu funcionamento.

[18] Segundo a NEP N.º AUOOS/DIP/02/05, de 30 de dezembro de 2014, ao abrigo do seu n.º 3, al. f), são definidas, anualmente, a nível estratégico

II.2.4 Policiamento Orientado pelas Informações

Antes de abordar o Policiamento Orientado pelas Informações (POI), também designado por *Intelligence Led Policing* (ILP), importa salientar que este modelo surge como desenvolvimento lógico do próprio conceito de inteligência aplicado à atividade policial, sobretudo num contexto marcado pela complexidade, pela incerteza e pela necessidade de apoiar a decisão com conhecimento útil e oportuno. Ao permitir antecipar padrões, riscos e oportunidades de intervenção, a análise e a fusão de dados colocam a informação no centro da ação policial (Pearsall, 2010). É precisamente essa valorização da informação que opera uma mudança de paradigma, deslocando o foco da polícia da mera reação ao crime consumado para a prevenção da criminalidade futura. Como consequência, os recursos podem ser distribuídos de forma mais eficiente e orientada para os contextos de maior risco (Fernandes, 2014).

O POI afirmou-se como resposta às limitações do policiamento tradicional, num contexto marcado pelo crescimento da criminalidade, pela pressão para utilizar menos recursos e pela perceção de que uma parte significativa dos crimes era cometida por um número relativamente reduzido de infratores (Peterson, 2005). Este desenvolvimento foi igualmente impulsionado por uma frustração crescente, tanto ao nível governamental como das chefias policiais, perante a subida dos índices criminais apesar do investimento realizado nas forças de segurança (Maguire & John, 2006).

A sua consolidação ficou fortemente associada a um conjunto de transformações estruturais no campo policial. Entre estas destacam-se a evolução tecnológica e a digitalização, que aumentaram a capacidade de recolha, armazenamento e tratamento de dados, bem como a expansão da criminalidade organizada e transnacional num contexto de globalização (Ratcliffe, 2008).

Nesta perspetiva, o POI é definido por Ratcliffe (2008)

> como um modelo de negócio e uma filosofia de gestão em que a análise de dados e a inteligência sobre a criminalidade são a pedra angular de um quadro decisório objetivo que facilita a prevenção e a redução da criminalidade através da gestão estratégica e da aplicação efetiva de estratégias que têm por alvo os criminosos prolíficos e os que cometem crimes graves. (p. 89)

Numa formulação posterior, o mesmo autor apresenta o POI como um modelo de gestão em que a análise de informações e a inteligência criminal ocupam uma posição central na tomada de decisão racional, com vista à redução dos problemas e da criminalidade, em especial da criminalidade grave e reincidente (Ratcliffe, 2008). Em sentido próximo, Carter & Carter

(2009) descrevem-no como um processo de recolha e análise de informação relacionada com o crime ou com o ambiente que o favorece, produzindo inteligência de valor acrescentado apta a apoiar o planeamento estratégico e as respostas táticas da organização policial.

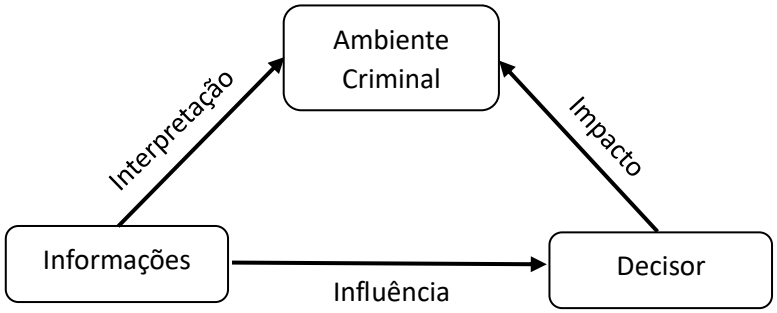
A literatura mostra que não existe uma definição universalmente aceite de POI. Essa ausência de consenso torna possível adaptar o modelo às especificidades de cada organização policial, desde que se preservem alguns traços comuns: centralidade da inteligência, orientação da estratégia e das operações, apoio à investigação e à prevenção criminal, priorização dos problemas mais relevantes e avaliação permanente dos resultados (Fernandes, 2014). Em Portugal, o estudo do POI não possui ainda uma definição correta e aplicação concreta. Ribeiro (2006) define-o como "um Modelo de Policiamento, suportado por uma Filosofia Policial no mesmo sentido" (p.21). Já Clemente (2009) entende-o como um "modelo de ação policial em que o produto informacional dirige o esforço de patrulhamento, para dissuadir a prática de incivilidades" (p. 97). Enquanto Elias (2022) sublinha a análise da informação como "componente central do pensamento estratégico", exigindo uma "interpretação abrangente de toda a informação recolhida pela Polícia" (p. 147).

Um dos pressupostos fundamentais do POI reside na ideia de que o crime não se distribui de forma aleatória. Ratcliffe (2003), descreve que o modelo integra quatro elementos essenciais: a definição de perfis de autores de crimes ou distúrbios, a gestão de *hotspots* de criminalidade e desordem, a investigação das ligações entre séries de crimes e incidentes e a aplicação de medidas preventivas.

Ao nível operacional, o POI assenta num processo contínuo de produção e utilização de informações. Cope (2004) identifica cinco etapas fundamentais: aquisição de informação, análise, revisão, ação e avaliação. Este processo tanto pode assumir uma lógica linear como funcionar em circuito de retroalimentação, aproximando-se de um verdadeiro ciclo de informações. Nesta medida, os analistas deixam de ocupar um lugar periférico e passam a integrar o núcleo da decisão policial, exigindo-se especialistas qualificados e ferramentas adequadas para explorar padrões, antecipar comportamentos e sustentar respostas mais eficazes (Tilley, 2005).

Figura 2

Modelo 3-i



Nota: Adaptado de "Intelligence-led policing", by J. Ratcliffe, 2003, p. 110

A representação gráfica mais conhecida deste modelo encontra-se no modelo 3-i de Ratcliffe (2003), ilustrado da Figura 2, que evidencia três vetores centrais: o ambiente criminal, a análise e a decisão. Segundo o autor, o ambiente criminal é descrito como dinâmico, fluido e em constante transformação, pelo que a sua interpretação exige estruturas capazes de recolher, tratar e analisar informação de forma contínua. A partir daí, os analistas interpretam esse ambiente, identificam ameaças, ofensores e tendências, influenciam os decisores e estes, por sua vez, através das decisões estratégicas e operacionais que adotam, influenciam novamente o ambiente criminal (Ratcliffe, 2008). Trata-se, portanto, de um modelo marcadamente *top-down*, no qual os comandantes definem prioridades, orientam recursos e avaliam continuamente o impacto das respostas desenvolvidas (Fernandes, 2014; Ratcliffe, 2008).

Em síntese, o POI distingue-se por procurar transformar informação dispersa em inteligência útil, capaz de orientar a organização policial para uma atuação mais seletiva, proativa e eficiente. A sua lógica não consiste apenas em acumular dados, mas em utilizar conhecimento analisado para identificar ameaças, antecipar comportamentos, concentrar recursos onde o risco é maior e avaliar continuamente os efeitos da intervenção policial.

II. 3. Complementaridade entre Ameaça e Risco

II. 3.1. Avaliação da Ameaça

Ao abordar o fenómeno da segurança pessoal, o ponto de partida tem de ser a clarificação do que entendemos por ameaça. Para Couto (1988), a ameaça corresponde a "qualquer acontecimento ou ação (em curso ou previsível) que contraria a consecução de um objetivo e que, normalmente, é causador de danos, materiais e morais" (p. 329). Em complemento, Escorrega (2009) sublinha que uma situação apenas se transforma numa verdadeira ameaça "se o seu agente tiver possibilidades ou capacidades para a sua

concretização e se também tiver intenções de a provocar" (p. 6). Deste modo, não basta existir um contexto potencialmente perigoso, é necessário que haja, em simultâneo, intenções hostis e meios concretos para as realizar.

Fernandes (2004) acrescenta duas dimensões decisivas. Em primeiro lugar, a ameaça não é um estado permanente, mas algo condicionado por circunstâncias específicas de tempo, lugar e contexto. Em segundo lugar, afirma que essa ameaça se corporiza "quando pelo menos um adversário tem a intenção de alterar o *status quo* a seu favor dispondo de poder para aplicar alguma forma de coação sobre o outro" (Fernandes, 2004, p. 461). Desta forma, revela-se necessário identificar, concretamente quem são os atores hostis, que objetivos perseguem, que meios têm ao seu dispor e que contexto lhes oferece oportunidades. É também por isso que Magalhães (2018) "afirma que as ameaças para serem credíveis não se podem cingir às intenções - que só por si são essencialmente de natureza subjetiva" (p.29), devendo abranger as possibilidades de materialização, entendidas como "manifestações materiais dos recursos e tecnologia disponível" (Fernandes, 2014, p. 19).

O PCCCOFSS define no seu capítulo 6 alínea a), nº 4 que a avaliação dos níveis de ameaça à segurança interna, incluindo no que respeita a instalações, pessoas e eventos, é da responsabilidade do SIS, sendo realizada com a colaboração do SIED e de outros órgãos de informações pertencentes às forças e serviços de segurança. Dentro deste sistema, o SIS ocupa uma posição central, em Portugal, como é definido pelo Artigo 2.º nº 3 da Lei n.º 50/2014 de 13 agosto, onde o legislador atribuiu a exclusividade em tal matéria ao consagrá-lo como "o único organismo incumbido da produção de informações destinadas a garantir a segurança interna e necessárias a prevenir a prática de atos que possam alterar ou destruir o Estado de direito constitucionalmente estabelecido".

No âmbito específico da segurança pessoal, também o PCCCOFSS descreve no seu capítulo 5 alínea b), nº 2 que a proteção de altas entidades assenta em operações planeadas e executadas tendo em conta o cargo desempenhado pela entidade, bem como o grau de ameaça previamente avaliado. Desta forma, e no âmbito desta investigação, segundo Magalhães (2018), é ao SIS que compete determinar o grau de ameaça que impende sobre o protegido, sendo este complementado pela "avaliação e gestão do risco no quadro da segurança pessoal a altas entidades e pessoas alvo de ameaça relevante (magistrados, testemunhas, etc.)" (p. 29). Ou seja, a classificação do grau de ameaça produzida pelo SIS é essencial, mas a decisão operacional sobre medidas de proteção exige que a PSP desenvolva a sua própria leitura, centrada na gestão e avaliação do risco concreto que impende sobre cada protegido.

No que respeita às altas entidades, torna-se evidente a necessidade de instrumentos que permitam traduzir a ameaça em níveis claros e partilhados entre diferentes atores. Adotou-se, assim a Recomendação do Conselho (2001/C 356/01) de 6 de dezembro de 2001, para padronizar as ameaças dirigidas a entidades nacionais ou internacionais através de uma escala comum de avaliação da ameaça. De notar que, como refere o E6 (2026), a atribuição do serviço de segurança pessoal depende sempre do grau de ameaça atribuído à entidade e à pessoa a proteger, podendo o serviço ser executado apenas por inerência do cargo quando o grau é reduzido e nem sequer é formalmente fixado. Sendo que é a partir do grau significativo (grau 3), que passa a existir um briefing específico, sendo o SIS a difundir, através do SSI, a existência de eventuais ameaças.

Figura 3

Escala de avaliação do Grau de Ameaça

N.º	Identificação	Classificação da Ameaça
1	Imediato	Existem informações seguras que indicam a preparação ou execução iminente de um atentado contra a entidade ou evento. Impõe-se a adoção imediata de medidas excecionais de segurança e eventual alteração do programa.
2	Elevado	Existem indícios consistentes de que indivíduos ou organizações dispõem de capacidade operacional e apoio logístico para realizar um atentado com resultados significativos, podendo a entidade constituir um alvo prioritário.
3	Significativo	O contexto internacional ou de segurança pode favorecer a ocorrência de um atentado, existindo agentes com meios e preparação para o concretizar. A partir deste nível justifica-se a implementação de segurança pessoal.
4	Moderado	Não existem indícios específicos de ameaça, embora o contexto geral aconselhe a adoção de medidas preventivas de segurança adequadas ao evento ou à entidade.
5	Reduzido	Não existem elementos que indiquem a possibilidade de um atentado, sendo suficientes as medidas normais de segurança e manutenção da ordem pública.

Z	Zulu	Assinala a ocorrência de atos hostis contra a entidade que não colocam diretamente em causa a sua vida ou integridade física (ex.: empurrões, arremesso de objetos).

Nota: Adaptado de Magalhães, 2018, p.30, com base no PCCCOFSS

A adoção deste tipo de escala responde à necessidade de simplificar e harmonizar a linguagem entre serviços, permitindo rapidamente situar o nível de ameaça em categorias como é visível na Figura 1. No entanto, segundo Magalhães (2018), acaba por ser informação complementar e limitada, não nos permitindo criar um quadro situacional mais completo. Tal como refere Torres (2015), esta escala "não está isenta de críticas, tendo em conta que, por um lado, quase ignora as componentes capacidade e intenções e centra-se praticamente no alvo e na oportunidade da ação hostil" (p. 36).

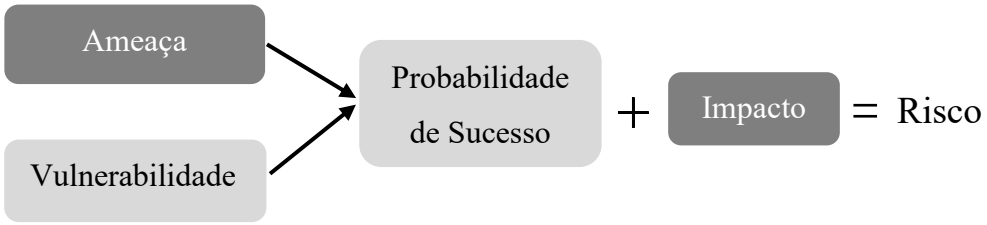
II. 3.2. Gestão do Risco

A mera identificação da ameaça não permite, por si só, determinar o nível de exposição de um determinado sistema ou entidade a possíveis danos. Para esse efeito, torna-se necessário introduzir o conceito de risco, que permite integrar a ameaça com outros fatores relevantes para uma avaliação da segurança mais completa. Como salientou o E3 (2026) "essa informação é-nos devolvida com a avaliação da ameaça […] e nós complementamos com uma avaliação do risco. Não é a mesma coisa, é complementar".

Neste sentido, o conceito de risco tem sido objeto de múltiplas formulações, procurando responder às necessidades de diferentes domínios científicos e profissionais. Nesse sentido, Torres (2015) define risco como a "probabilidade de uma determinada ameaça explorar com sucesso uma vulnerabilidade potencial do sistema resultando um determinado impacte num ativo crítico para a missão e objetivos de uma empresa, instituição ou Estado" (p. 9). Esta definição evidencia que o risco não resulta apenas da existência de uma ameaça, mas da possibilidade concreta de esta vir a explorar fragilidades existentes num determinado sistema, produzindo efeitos negativos sobre ativos considerados essenciais. Neste sentido, o conceito de risco assenta na articulação de duas variáveis fundamentais: (1) a probabilidade de concretização de uma determinada ameaça e (2) o impacto que a sua eventual ocorrência pode produzir, quer no curto prazo, quer no médio e longo prazo (Torres, 2015). A figura 4 ilustra como a primeira variável corresponde à relação estabelecida entre o grau específico da ameaça identificada e o nível de vulnerabilidades existentes perante essa mesma ameaça.

Figura 4

Sistematização do risco



Nota: Adaptado de Torres (2018)

Como se interpreta, pode assim existir um elevado risco com uma ameaça baixa porque o impacto é proporcionalmente muito grande. Ou um baixo risco com ameaça elevada, derivado de um impacto muito reduzido (Torres, 2015).

No âmbito desta investigação, com uma clara orientação para a prática técnico-operacional, adota-se, contudo, a conceptualização apresentada por Fernandes (2014), que enquadra o risco numa perspetiva particularmente adequada ao domínio da segurança. De acordo com este autor, o risco corresponde a uma "função da antecipação das consequências decorrentes da materialização de uma ameaça que explora um conjunto de vulnerabilidades, num determinado período de tempo, relativamente a um ativo" (Fernandes, 2014, p. 22). Assim, o risco pode ser entendido como o resultado da interação entre diferentes elementos como a ameaça e as vulnerabilidades existentes, cuja conjugação determina a probabilidade de ocorrência, e as consequências associadas à eventual concretização da ameaça.

Perante a inevitabilidade da existência de riscos, assume particular relevância o desenvolvimento de processos sistemáticos destinados à sua gestão. Segundo Hopkin (2018), a gestão do risco corresponde ao conjunto de procedimentos através dos quais uma organização procura identificar, compreender e classificar os riscos que podem afetar a prossecução dos seus objetivos, tendo sempre em consideração a sua estratégia institucional e o contexto em que opera.

Desta forma, a gestão do risco deve ser entendida essencialmente como um instrumento de apoio à tomada de decisão. Tal como sublinha Torres (2015), trata-se de um processo que permite ao decisor dispor de informação estruturada sobre as diferentes opções disponíveis, bem como sobre as respetivas vantagens e desvantagens para a organização, numa lógica de análise custo-benefício.

Importa igualmente referir que as práticas contemporâneas de gestão do risco são fortemente influenciadas pelas orientações estabelecidas na norma ISO 31000 (2018), que

define princípios e diretrizes aplicáveis à gestão do risco nas organizações. Embora esta norma esteja particularmente orientada para o posicionamento estratégico das instituições, a gestão do risco assume igualmente relevância na concretização de objetivos e projetos em diferentes níveis organizacionais. Consequentemente, trata-se de uma atividade transversal, que atravessa a organização tanto numa lógica descendente, do nível estratégico para o operacional, como numa lógica ascendente, envolvendo os níveis estratégico, operacional e tático (Rodrigues, 2025).

No domínio específico da segurança, a gestão do risco envolve também uma dimensão relacionada com a perceção de segurança. Conforme refere Torres (2015), importa distinguir entre o risco objetivo, resultante de uma análise técnica das ameaças e vulnerabilidades, e a perceção subjetiva desse risco por parte dos indivíduos ou das organizações.

Apesar da sua frequente associação no discurso corrente, ameaça e risco constituem conceitos distintos do ponto de vista analítico. Como referem Fernandes (2014) e Torres (2015), o risco resulta de um processo de construção analítica que integra diferentes variáveis, entre as quais se encontra a própria ameaça. Por conseguinte, não é metodologicamente correto colocar ambos os conceitos no mesmo plano conceptual.

Neste contexto, Torres (2015) defende que o processo de avaliação dos riscos de segurança deve iniciar-se com a identificação dos ativos críticos que necessitam de proteção. Segundo o autor, "para planear segurança há que ter a exata ideia do que é preciso proteger e/ou salvaguardar" (Torres, 2015, p. 24). A definição desses ativos constitui, assim, o ponto de partida para qualquer processo de avaliação de risco, permitindo orientar posteriormente a análise das ameaças e das vulnerabilidades associadas.

No que respeita à tipologia desses ativos, Torres (2015) identifica diferentes categorias, entre as quais se destacam, desde logo, as entidades, cuja proteção assume particular relevância no contexto das políticas de segurança e na vertente da segurança pessoal.

Assim, a análise do risco corresponde ao momento em que se desenvolve uma abordagem analítica aprofundada, baseada na recolha e interpretação de informação relevante que permita caracterizar adequadamente as ameaças, identificar vulnerabilidades e antecipar as consequências da eventual materialização de determinados eventos adversos (Rodrigues, 2025).

Devido à grande quantidade de dados disponíveis, tanto em fontes abertas como classificadas, como falado anteriormente, torna-se necessário direcionar a análise para tipologias de risco que possam ter maior impacto no contexto específico em análise. De acordo

com Rodrigues (2025), esta orientação permite identificar alterações significativas entre diferentes eventos, integrar informação histórica e atual e produzir inteligência capaz de apoiar o planeamento operacional.

No domínio da atividade policial, a gestão do risco assume particular relevância enquanto ferramenta de apoio ao planeamento e à tomada de decisão. De acordo com Magalhães (2018), esta abordagem permite ultrapassar uma perspetiva limitada centrada exclusivamente na determinação do grau de ameaça. Pelo contrário, a gestão do risco na atividade policial integra um conjunto mais alargado de fatores analíticos, incluindo as intenções e capacidades dos potenciais agentes hostis, as vulnerabilidades identificadas e a probabilidade de ocorrência de incidentes. No âmbito da segurança pessoal, o E3 (2026) descreve que "o objetivo é colecionar, recolher tudo o que tenha acontecido sobre aquela pessoa, o histórico passado, coisas que poderão eventualmente levar-nos a considerar uma avaliação do risco".

Segundo Felgueiras (2015), é precisamente a articulação entre inteligência, conhecimento científico e experiência profissional que permite desenvolver modelos de gestão estratégica do policiamento adequados às especificidades de cada situação. Como refere o autor:

> Para o sucesso de uma operação policial não basta a quantidade, qualidade, atualidade e pertinência da informação disponível, é fundamental que os decisores tenham conhecimento adequado sobre os fenómenos identificados, para interpretar, antever e antecipar estratégias que limitem os fatores de risco presentes nos acontecimentos. (Felgueiras, 2015, p. 6)

Simultaneamente, esta abordagem fornece ao comandante tático elementos essenciais para a definição e implementação de medidas de segurança adequadas à missão, quer no plano preventivo quer no plano reativo (Magalhães, 2018).

II. 4. Planeamento e Cenarização na Segurança Pessoal

II.4.1. Novo paradigma Criminal e Grau de Incerteza

Antes de mais, importa assinalar que o presente subcapítulo se apoia, em larga medida, numa linha doutrinária ainda em desenvolvimento, não totalmente consolidada no plano académico. Não obstante essa limitação, a sua incorporação revela-se fundamental para compreender a transformação do ambiente securitário contemporâneo e, sobretudo, para estabelecer uma ponte com os desafios específicos da segurança pessoal. Neste sentido, a

natureza emergente destes contributos não diminui a sua relevância, pelo contrário, reflete a necessidade de adaptar o pensamento científico a uma realidade em rápida mutação.

Os desenvolvimentos recentes no panorama securitário internacional, marcados por ataques violentos perpetrados em diversas cidades do mundo ocidental, refletem uma transformação profunda na natureza da ameaça contemporânea. Segundo Torres (2018), estes episódios, frequentemente dirigidos de forma indiscriminada contra populações civis ou grupos profissionais específicos, como forças de segurança e militares, apontam para a emergência de uma nova realidade criminológica caracterizada pela difusão do terror e, nomeadamente, pela imprevisibilidade da ação violenta. Tal contexto impõe uma reconfiguração abrangente das abordagens tradicionais, desde o plano político-estratégico até ao nível tático-operacional, onde atuam diretamente as FSS (Torres, 2018).

Apesar do reforço significativo das medidas de segurança adotadas pelos Estados, como o aumento da vigilância sobre indivíduos radicalizados ou em processo de radicalização, a intensificação da cooperação internacional em matéria de informações, o reforço do controlo de fronteiras e a maior presença policial no espaço público, subsiste uma dificuldade estrutural na contenção deste fenómeno. Tal dificuldade decorre, em grande medida, da natureza difusa e frequentemente individualizada das ameaças, que podem materializar-se através de agentes isolados, sem ligações formais a organizações e com processos de radicalização autónomos.

Como explica Torres (2018), é neste ponto que surgem os fenómenos dos "*active shooters"* e dos denominados "lobos solitários", assumindo estes últimos particular relevância para uma análise da eficácia operacional na segurança pessoal. Estes indivíduos, ao atuarem de forma isolada, com baixos níveis de exposição prévia e recorrendo frequentemente a meios acessíveis, introduzem um grau de imprevisibilidade que compromete seriamente os modelos clássicos de proteção. No contexto do CSP, esta nova realidade traduz-se na dificuldade em antecipar ameaças concretas com base em perfis ou padrões comportamentais, exigindo uma adaptação das metodologias de avaliação e atuação. A inexistência de sinais claros ou de ligações a redes estruturadas reduz drasticamente a eficácia de abordagens assentes exclusivamente na inteligência preditiva, contribuindo para a consolidação de um nível de risco elevado, isto é, um risco que não pode ser plenamente identificado, quantificado ou controlado (Torres, 2018).

No plano conceptual, para Torres (2015), a caracterização das "ameaças intencionais" assenta, tradicionalmente, em três vetores fundamentais: desejos e expetativas (intenções), capacidades (recursos) e oportunidades (p.21). Entre estes, as intenções do agente acabam por

constituir o elemento mais difícil de apreender, mesmo em contextos onde existem mecanismos de *intelligence* e contrainformação. Quando se trata de indivíduos isolados como mencionados anteriormente, essa dificuldade intensifica-se exponencialmente, sendo que para a segurança pessoal, esta limitação é particularmente crítica, pois impede a identificação antecipada de ameaças direcionadas às entidades protegidas.

A realidade portuguesa ilustra, de forma particularmente evidente, os desafios associados à avaliação da ameaça terrorista. A inexistência de ocorrências relevantes em território nacional tem contribuído para uma perceção generalizada de baixo risco, frequentemente enquadrada na lógica do chamado "cisne negro", um evento de reduzida probabilidade, mas de elevado impacto (Torres, 2018). Esta perspetiva tende a alimentar uma certa inércia estratégica, assente numa expectativa implícita de que, apesar da necessidade de vigilância, a materialização de um ataque significativo permanece improvável.

Para melhor entender este novo fenómeno criminal, importa também a distinção entre segurança objetiva e segurança subjetiva. Conforme argumenta Zedner (2009), a segurança pode ser entendida, por um lado, como a ausência efetiva de ameaças e, por outro, como a ausência de perceção de insegurança, traduzida em sentimentos como medo ou ansiedade. Torres (2018) sublinha a relevância desta dicotomia, destacando que, embora as políticas de segurança tendam a privilegiar a dimensão objetiva, através da redução efetiva dos riscos, a componente subjetiva assume igualmente um papel determinante, dispondo o estado de "um vasto leque de medidas de maior visibilidade, ou, em oposição, de recato, silenciosas, mas não menos efetivas" (p. 28).

Contudo, continua a subsistir a impossibilidade de eliminação total do risco, e nesta ideia, Torres (2018), descreve a existência de um "risco estrutural" (p. 20) que permanece ativo e não é controlável, refletindo a incapacidade de antecipar todas as ameaças, identificar todas as vulnerabilidades e garantir a eficácia absoluta das contramedidas adotadas. Para a segurança pessoal, isto traduz-se na necessidade de aceitar a inevitabilidade de exposição ao risco, orientando a ação para a sua redução e não para a sua eliminação.

A complexidade do fenómeno agrava-se quando se consideram as características do terrorismo contemporâneo, em particular o de matriz islâmica. Segundo Torres (2018) a multiplicidade de potenciais agentes, a ausência de perfis-tipo consistentes e a ocorrência de ataques perpetrados por indivíduos fora do radar das FSS e dos Serviços de Informações dificultam significativamente os processos de deteção e prevenção. Como evidenciado por Rego (2017), muitos destes atores, caracterizados por "lobos solitários" apresentam trajetórias

atípicas, podendo agir de forma autónoma, ainda que influenciados à distância por estruturas ideológicas ou redes informais. Esta realidade compromete a capacidade dos sistemas de segurança para operar numa lógica preditiva sustentada, baseada na identificação de padrões, uma limitação particularmente relevante para a segurança pessoal, onde a antecipação de ameaças direcionadas é um objetivo central.

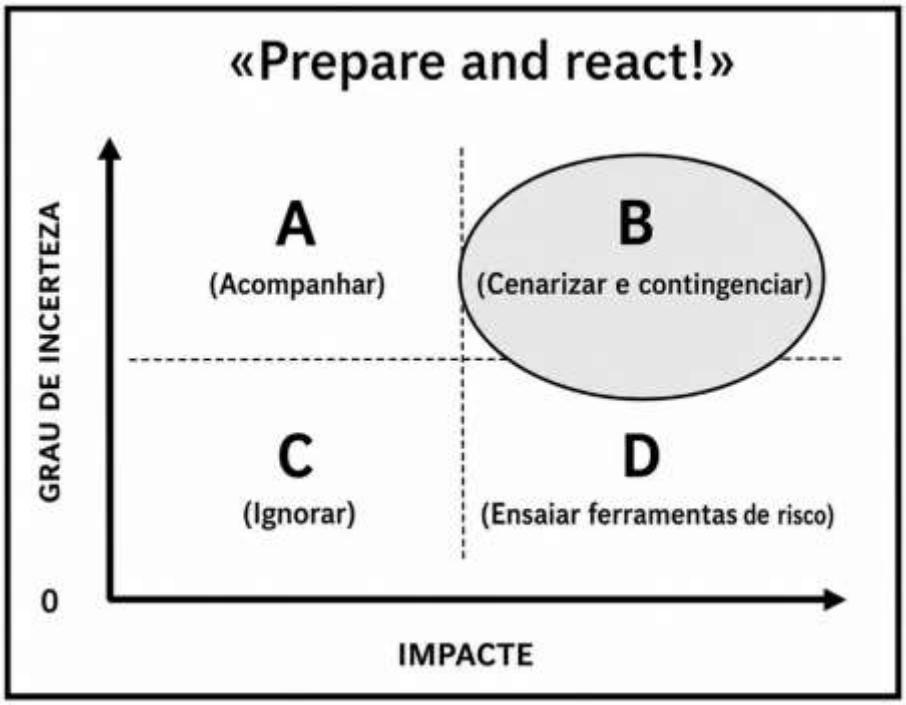
É neste contexto de imprevisibilidade que Torres (2018) conclui que existe uma transição de um paradigma de gestão do risco para um paradigma de gestão da incerteza e, portanto, importa sublinhar que a avaliação da ameaça não segue necessariamente a mesma lógica metodológica que caracteriza a avaliação do risco. Neste contexto, Torres (2018) propõe uma distinção conceptual entre a gestão do risco e a gestão da incerteza. De acordo com este autor,

> a grande diferença entre gerir o risco e a incerteza é que, na primeira situação, existindo obviamente incerteza no sentido lato do termo, os fatores que introduzem a aleatoriedade na 'equação' são conhecidos, traduzindo-se por um grau qualitativo ou por um valor quantitativo de probabilidade de ocorrência de uma ameaça. Já quando se gere a incerteza, em sentido restrito, atuamos num contexto de puro desconhecimento da ameaça, em que nem sequer é possível aferir os fatores de aleatoriedade que determinam o resultado final. (p. 24)

Deste modo, acaba por se sintetizar, se o gestor de risco tende a concentrar-se nos cenários mais prováveis e de maior impacto, o gestor da incerteza orienta a sua atenção para cenários altamente incertos, mas igualmente potencialmente disruptivos (Torres, 2018). Esta mudança de foco traduz uma adaptação às características do ambiente atual, onde a imprevisibilidade se assume como traço dominante.

Figura 5

Estratégias típicas de gestão da incerteza



Nota: Adaptado de Torres, 2018, p. 24

Atendendo à figura 5 apresentado, o quadrante destacado é o que assume particular relevância para a segurança pessoal, na medida em que conjuga elevado grau de incerteza com elevado impacto, constituindo o espaço privilegiado de atuação do gestor da incerteza (Torres, 2018). Neste domínio inserem-se fenómenos como os ataques perpetrados por "*active shooters*" ou "lobos solitários", já abordados, em que a ameaça é pouco conhecida ou mesmo indeterminável, inviabilizando abordagens clássicas centradas na previsão. Consequentemente, transita-se de uma lógica preventiva, assente na identificação de ameaças e vulnerabilidades, para uma lógica predominantemente adaptativa e reativa, sintetizada no princípio *"Prepare and react"*.

No plano tático-operacional, particularmente no *modus operandi* do CSP, esta atuação deve ser entendida predominantemente sob a ótica da incerteza, deixando de se basear prioritariamente na neutralização antecipada da ameaça, passando a privilegiar a preparação para a sua eventual materialização. Neste sentido, a resposta deverá centrar-se, sobretudo, na mitigação dos impactos, na capacidade de reação imediata e na reposição célere da normalidade. Como refere Torres (2018), a gestão da incerteza implica uma postura tendencialmente mais reativa, em contraste com a lógica preventiva associada à gestão do risco.

Perante este enquadramento, marcado por elevados níveis de incerteza e pela limitação das abordagens tradicionais de antecipação, torna-se necessário repensar os instrumentos de apoio à decisão no contexto operacional da segurança pessoal. Neste sentido, ganha particular relevância a adoção de metodologias assentes na cenarização, enquanto forma de estruturar a resposta a múltiplas possibilidades plausíveis, permitindo ao CSP preparar-se não para uma ameaça específica, mas para diferentes formas de materialização do risco.

II.4.2 Modelo DIDRA e Cenarização na Segurança Pessoal

Perante um contexto securitário marcado pela imprevisibilidade e pela limitação das abordagens puramente preditivas, torna-se necessário operacionalizar modelos que permitam estruturar a atuação das forças de segurança, nomeadamente no domínio da segurança pessoal. Neste sentido, o modelo DIDRA, proposto por Torres (2024), apresenta-se como uma ferramenta conceptual com aplicação particularmente relevante neste âmbito, na medida em que sistematiza os principais pilares de um sistema protetivo eficaz, assente nos elementos-chave: Dissuasão, Interdição, Deteção, Resposta e Adaptação.

Figura 6

Modelo DIDRA

Nota: Adaptado de Torres, 2024, p.59

O objetivo central de qualquer dispositivo de segurança pessoal consiste, em última instância, em impedir que uma ameaça se concretize com sucesso, sendo desejável que esta nem sequer chegue a materializar-se. Tal pressupõe uma clara primazia da dimensão preventiva sobre a repressiva, ainda que, no atual paradigma de incerteza, essa prevenção não possa assentar exclusivamente na antecipação, mas sim na construção de um sistema resiliente e multifuncional. Esta base conceptual vem no seguimento das palavras de Torres (2018), quando descreve que

> o objetivo último de um qualquer sistema protetivo passa por evitar que uma determinada ameaça seja bem-sucedida. Acima de tudo, o ideal é que esta nem sequer esboce uma tentativa para o fazer, apostando no fator preventivo, em detrimento do repressivo (p. 27).

O primeiro elemento do modelo DIDRA, a dissuasão, assume particular importância no contexto da segurança pessoal. Este traduz-se na criação de uma perceção de inacessibilidade ou invulnerabilidade do alvo, ainda que parcialmente construída, através da projeção de sinais de segurança visíveis, de natureza física, humana ou tecnológica (Torres, 2024). No âmbito do CSP, esta lógica materializa-se, por exemplo, na presença ostensiva de equipas de proteção, na adoção de dispositivos de segurança visíveis em eventos ou deslocações, e na utilização de medidas que reforcem a perceção de controlo do espaço.

Contudo, a dissuasão não se esgota na dimensão visível. No âmbito e no interesse desta investigação, mas também numa lógica mais ampla de integração entre informações e operações, assume particular relevância a eventual utilização de equipas especializadas de atuação encoberta, como as Equipas de Reação Tática Encobertas (ERTE). Estas equipas foram inicialmente conceptualizadas na PSP a partir da proposta de criação das Equipas de Deteção e Reação Encoberta (EDRE) em 2004, vindo o conceito a evoluir no seio do Departamento de Operações para as atuais ERTE. A sua génese assenta, assim, numa lógica de resposta a ameaças altamente dinâmicas e imprevisíveis, exigindo soluções operacionais igualmente flexíveis e dissimuladas.

De acordo com Torres (2018), estas equipas atuam de forma encoberta em teatros de operações de maior risco, incluindo missões de operações especiais e de segurança pessoal, integrando-se de forma impercetível no ambiente envolvente e mantendo capacidade de intervenção imediata, proporcional ao nível de ameaça. Dotadas de competências especializadas como técnicas de disfarce, vigilância, *close combat*, recolha de informações e contrainformação, as ERTE representam um dos núcleos mais reservados e tecnicamente preparados da UEP. Para além da sua vertente operacional, a sua mera existência constitui um relevante fator dissuasor, ao introduzir incerteza no potencial agressor quanto à presença e capacidade de resposta das forças de segurança.

Mais do que um instrumento tático, estas equipas materializam, de forma clara, um modelo híbrido entre informações e operações, permitindo não só recolher dados em ambiente real, mas também intervir de forma imediata sobre ameaças emergentes. Esta lógica que, como referido por Torres (2020), assenta na "infiltração no ambiente de operações de equipas

dissimuladas de reação imediata" (p. 16), enquadra-se na necessidade, anteriormente identificada, de responder à "imprevisibilidade da ameaça com uma igual imprevisibilidade da resposta (Torres, 2020, p.16). Neste sentido, as ERTE contribuem para operacionalizar uma abordagem adaptativa, característica da gestão da incerteza, reforçando simultaneamente os pilares da dissuasão, deteção e resposta no modelo DIDRA.

Caso a dissuasão não seja suficiente, entramos no segundo elemento-chave do modelo, a interdição. Segundo Torres (2018), este traduz-se na implementação de medidas destinadas a impedir, atrasar ou condicionar a ação da ameaça, através de soluções de natureza diversa, incluindo barreiras físicas, controlo de acessos, procedimentos de segurança e dispositivos humanos e tecnológicos. No contexto da segurança pessoal, a interdição assume especial relevância em ambientes controlados, como eventos ou deslocações previamente planeadas, onde é possível incidir numa possível estruturação do espaço de forma a limitar oportunidades de ação hostil.

O terceiro elemento, a deteção e avaliação, corresponde à capacidade de identificar precocemente sinais de ameaça, permitindo a sua avaliação e a ativação de respostas adequadas. Neste domínio, assume particular importância a integração de sistemas de vigilância, análise comportamental, recolha e tratamento de informação, bem como a articulação de informações entre diferentes fontes (Torres, 2024). No contexto do CSP, a deteção de uma ameaça de forma precoce pode fazer a diferença entre uma situação controlada e um incidente crítico, sendo especialmente desafiante em cenários de elevada incerteza, como os associados a agentes isolados.

Segue-se a resposta, que, em ambientes marcados pela imprevisibilidade, como os descritos no subcapítulo anterior, tende frequentemente a assumir um papel central. A resposta consiste na capacidade de atuação imediata face à materialização da ameaça, envolvendo os chamados *first responders*, tanto na vertente do *safety* como do *security* (Torres, 2018). No âmbito da segurança pessoal, esta dimensão traduz-se na capacidade de as equipas no terreno reagirem de forma rápida, proporcional e eficaz, garantindo sempre a salvaguarda da entidade protegida e a neutralização da ameaça.

Este elemento articula-se com o conceito de "Segurança Just-In-Time" introduzido por Torres (2011), que assenta numa lógica de elevada mobilidade, flexibilidade e projeção de meios em função da necessidade concreta. Ao invés de uma presença massiva e estática, privilegia-se a capacidade de concentrar recursos no momento e local adequados, suportada por sistemas de informação, comando e controlo eficientes.

Por fim, o modelo DIDRA integra o elemento-chave da adaptação, que assume um papel estruturante num ambiente caracterizado pela constante evolução das ameaças. Este elemento implica a reavaliação contínua dos dispositivos de segurança, com base na análise de incidentes, identificação de vulnerabilidades e incorporação de lições aprendidas (Torres, 2018). No contexto da segurança pessoal, a adaptação traduz-se na necessidade de atualização permanente de procedimentos, treino e metodologias, bem como incidência na melhoria da coordenação entre diferentes entidades, nomeadamente entre FSS.

Paralelamente, importa destacar o papel da cenarização enquanto instrumento transversal ao modelo DIDRA. Como cenários entendemos

> narrativas estruturadas representativas de futuros possíveis, descrevendo sequências plausíveis de acontecimentos relativos a hipóteses de evolução de uma situação de origem a uma situação futura, para um dado horizonte temporal, tendo por base a identificação e análise das principais forças de influência suscetíveis de conferirem novas dinâmicas e direções de evolução. (Carvalho, 2016, p.16)

Tanto na gestão do risco como na gestão da incerteza, o planeamento contingencial assenta na construção de cenários e subcenários relevantes para o decisor, aos quais são associadas contramedidas específicas (Torres, 2015). No entanto, é necessário ter em consideração que em

> contextos de gestão de riscos o exercício de cenarização é muito mais concreto e objetivo – a ameaça está bem melhor configurada –, na gestão da incerteza o ensaio de cenarização obedece a critérios muito mais genéricos e abrangentes, o que, à partida, também o torna menos efetivo e proveitoso no plano tático-operacional. (Torres, 2024, p. 65)

Consideramos que no âmbito do CSP, a cenarização não deve procurar prever eventos específicos, mas antes preparar as equipas para um conjunto diversificado de possibilidades, valorizando a capacidade de adaptação, o treino e a flexibilidade dos operacionais. Em cenários marcados por agentes isolados e imprevisíveis, o fator improviso e a pronta resposta operacional tornam-se elementos críticos, reforçando a importância de um sistema que vá além da antecipação e se centre na capacidade de resposta eficaz.

II. 5. Contrainteligência e Desinformação na Perceção Situacional

II.5.1. Conceito Contrainteligência e Desinformação

A contrainteligência, também designada no nosso contexto institucional como contrainformação, constitui uma dimensão essencial da atividade de *intelligence*, considera-se relevante abordar este tópico nesta investigação, constituindo-se também uma pergunta derivada nesse sentido.

> Na literatura clássica, e de acordo com Lowenthal (2009), a contrainteligência refere-se aos esforços empreendidos para proteger as próprias operações de *intelligence* contra a infiltração e a perturbação levadas a cabo por nações hostis ou pelos seus serviços de informações […] informação recolhida e atividades realizadas para identificar, enganar, explorar, neutralizar ou proteger contra a espionagem e outras atividades levadas a cabo por Estados estrangeiros ou atores não estatais.[19] (p. 151)

Esta definição evidencia, desde logo, a amplitude do conceito, que abrange simultaneamente dimensões defensivas e ofensivas. Não se limita à proteção passiva, integrando igualmente um conjunto de atividades de natureza operacional orientadas para a identificação, neutralização e exploração de ameaças.

Neste âmbito, Lowenthal (2020) identifica três grandes categorias de contrainteligência: (i) a vertente da recolha, que visa obter informação sobre as capacidades de *intelligence* do adversário; (ii) a vertente defensiva, orientada para impedir os esforços de serviços de *intelligence* hostis se infiltrem no próprio sistema; e (iii) a vertente ofensiva, que procura explorar as ações adversárias, por exemplo através da utilização de agentes duplos ou da disseminação de informação enganosa. Esta tipologia reforça a ideia de que a contrainteligência ultrapassa largamente uma função meramente reativa, assumindo um papel ativo na modelação do ambiente informacional.

No plano conceptual, Lowenthal (2020) invoca também a ideias de dois autores e antigos membros da *Central Intelligence Agency* (CIA) com experiência na área da contrainteligência. Segundo Redmond (2010), define a contrainteligência como um conjunto alargado de atividades destinadas a apoiar os próprios esforços e a contrariar os do adversário, incluindo ações como a contraespionagem, a validação de fontes HUMINT, a desinformação e o desenvolvimento de técnicas operacionais. Por sua vez, Ehrman (2009) entende a contrainteligência como "o estudo da organização e do comportamento dos serviços de

[19] Tradução livre do autor

informações de Estados e outras entidades, bem como a aplicação do conhecimento daí resultante"[20] (p. 2).

No contexto institucional português, a contrainteligência encontra expressão no SIRP, designadamente através do SIS, cuja missão, como já abordado, inclui a prevenção de ameaças como o terrorismo, a espionagem e a sabotagem, recorrendo, entre outros instrumentos, a atividades de contrainteligência. Neste sentido, Fernandes (2014) define contrainteligência como

> atividades que têm por fim identificar e neutralizar as ameaças e riscos à segurança, provocadas por organizações ou indivíduos envolvidos em atividades destinadas a conhecer as atividades ou a sabotar ou neutralizar operações do Estado português destinadas a identificar e neutralizar riscos à segurança interna. (p. 90)

Por fim, importa sublinhar que, num contexto contemporâneo caracterizado pela intensificação da atividade de inteligência a nível global, pelo aumento das ameaças híbridas e pela crescente relevância do ciberespaço, a contrainteligência assume uma importância acrescida. Como observa Lowenthal (2020), tem-se verificado um aumento significativo das atividades de inteligência hostis, quer ao nível humano (HUMINT), quer no domínio cibernético, o que reforça a centralidade da contrainteligência enquanto instrumento essencial de proteção e antecipação.

Relativamente à desinformação, esta constitui uma das expressões mais sofisticadas da vertente ativa da contrainteligência, traduzindo-se na disseminação deliberada de informação falsa, manipulada ou descontextualizada com o objetivo de influenciar perceções, decisões e comportamentos.

Segundo Rid (2021), a desinformação deve ser enquadrada no conceito de "*active measures*". O autor sublinha ainda a dificuldade inerente à sua identificação, referindo que "reconhecer uma *active measure* pode ser difícil. A desinformação, quando bem executada, é difícil de detetar, sobretudo no momento em que se torna pública" (Rid, 2021, p. 9)[21]. Acrescenta também que "a desinformação não se resume simplesmente a informação falsa […] sendo que algumas das *active measures* mais eficazes da história foram concebidas para transmitir informação totalmente verdadeira"[22] (Rid, 2021, p.10). Esta perspetiva mostra que a

[20] Tradução livre do autor
[21] Tradução livre do autor
[22] *Idem*

desinformação não se limita a alterar ou distorcer factos, funcionando como uma estratégia de influência sobre o ambiente informacional.

No contexto europeu, a desinformação tem vindo a ser reconhecida como uma ameaça híbrida. A European Comission (2018) define-a como "informação comprovadamente falsa ou enganadora que é criada, apresentada e divulgada para obter vantagens económicas ou para enganar deliberadamente o público, e que é suscetível de causar um prejuízo público" (p. 4), destacando o seu potencial para afetar a segurança interna e a confiança nas instituições.

Importante também introduzir aqui o conceito da contravigilânica, que segundo McGovern (2011) "É uma técnica utilizada sobretudo por operacionais de *intelligence* para explorar o adversário após a deteção de uma presença hostil."[23] (p. 138). Apresenta-se assim como uma das medidas mais eficazes de contrainformação e com aplicação prática na segurança pessoal, pois visa detetar ações hostis de recolha de informação no terreno sobre a entidade.

Desta forma, a desinformação assume uma natureza ambivalente: sendo uma ameaça quando utilizada por atores adversários, pode também constituir um instrumento legítimo no âmbito da contrainteligência, desde que utilizada de forma controlada, proporcional e legalmente enquadrada, nomeadamente para a proteção de operações sensíveis ou para a indução de incerteza no potencial adversário.

II.5.2 Contrainformação e Desinformação na Segurança Pessoal

Aplicam-se agora os conceitos de contrainteligência e desinformação no domínio da segurança pessoal com o objetivo de destacar uma dimensão frequentemente subvalorizada desta atividade, pois a gestão do ambiente informacional é também um fator crítico na proteção de altas entidades.

Desde logo, verifica-se que, na prática operacional, segundo os contributos dos entrevistados, que existem alguns mecanismos que se aproximam de uma prática de contrainteligência, ainda que não formalizados como tal. O E1 (2026) refere, a este propósito, que podem ser adotadas práticas como a transmissão de informação incompleta ou a alteração de elementos operacionais divulgados, nomeadamente itinerários ou horários, com o objetivo de "reduzir vulnerabilidades" e "antecipar situações potencialmente prejudiciais". O mesmo conclui que estas práticas têm um objetivo operacional claro e legítimo pois não se trata de "enganar por si só" mas sim de proteger a informação da operação.

[23] Tradução livre do autor

De forma complementar, a gestão do timing da divulgação da informação é uma prática particularmente relevante. O E5 (2026) destaca que existe uma preocupação em limitar a antecedência da divulgação pública das deslocações, assim como dos itinerários procurando "dar a conhecer o mais próximo possível na véspera e não […] com vários dias de antecedência" (E5, 2026).

Todavia, os dados evidenciam que estas práticas assumem um carácter predominantemente empírico e não estruturado. O entrevistado E4 (2026) refere explicitamente que "não estão identificadas […] práticas no âmbito da contrainformação ou desinformação" no CSP, sublinhando que, na maioria dos casos, a atuação se centra na proteção da informação sensível que depende diretamente das equipas, como itinerários ou opções operacionais (E4, 2026). Esta ausência de formalização sugere a inexistência de uma doutrina consolidada nesta área, sendo que aplicação de práticas neste sentido acaba por ficar dependente da experiência individual dos operacionais.

Numa perspetiva crítica relativamente à aplicabilidade da desinformação no contexto da segurança pessoal de altas entidades, o E5 (2026) é claro ao afirmar que "não podemos dizer à comunicação social que a entidade vai a um sítio e afinal vai a outro", o que demonstra os limites operacionais associados à utilização de estratégias de desinformação. Esta posição é corroborada pelo E6 (2026), que considera que a contrainformação terá uma aplicabilidade mais reduzida neste contexto, podendo fazer mais sentido em cenários específicos, como a proteção de testemunhas ou situações de maior sensibilidade.

Neste sentido, consideramos que no contexto do CSP, a contrainteligência se materializa sobretudo através de medidas preventivas e defensivas, mais do que através de estratégias ativas de desinformação. O E1 (2026) sintetiza esta ideia ao referir que a adoção de medidas preventivas, como a não divulgação antecipada de agendas, a proteção de itinerários ou o armazenamento seguro de viaturas, "inibe a necessidade de se ter ações de desinformação ou outras medidas alternativas", uma vez que o risco é mitigado à partida.

Ainda assim, alguns contributos apontam para a relevância de práticas mais próximas da vertente ativa da contrainteligência. O E2 (2026) destaca, por exemplo, "desenvolvimento e aprimoramento de ações de contravigilância e de contramedidas face a ciberameaças e tecnológicas carecem de constante reforço", sublinhando o papel destas medidas na mitigação de vulnerabilidades associadas à exposição digital, e fazendo referência à questão da contravigilância, abordada no subcapítulo anterior. Aliás, também a dimensão cibernética surge como um dos principais desafios emergentes, como destaca também Rid (2021) ao

descrever que "A internet não trouxe maior precisão à arte e à ciência da desinformação — tornou as medidas ativas menos controladas: mais difíceis de gerir, de orientar e de circunscrever aos efeitos pretendidos. Como resultado, a desinformação tornou-se ainda mais perigosa."[24] (p. 14).

Por outro lado, alguns entrevistados defendem que a contrainteligência, enquanto função estruturada, não deverá ser integralmente assumida pelo CSP, mas antes desenvolvida de forma articulada com estruturas especializadas. O E3 (2026), por exemplo, entende que esta dimensão deverá funcionar como uma componente complementar, assegurada por serviços de inteligência que operam "nas costas" da segurança pessoal, garantindo uma camada adicional de proteção não visível.

Em síntese, podemos concluir que a contrainteligência já se encontra parcialmente incorporada nas práticas operacionais do CSP, embora de forma pouco estruturada. Assim, mais do que desenvolver estratégias complexas de desinformação, importa priorizar neste momento o reforço e a organização das práticas já existentes, sobretudo ao nível da gestão da informação, da antecipação de ameaças e da redução da previsibilidade, tornando o modelo mais eficaz e ajustado às atuais exigências.

[24] Tradução livre do autor

Capítulo III: A Integração Operacional da Inteligência Policial no Corpo de Segurança Pessoal

Neste último capítulo será feita a análise e discussão dos resultados provenientes das entrevistas elaboradas a polícias com funções e experiência nas valências de segurança pessoal e de informações na PSP. O objetivo é confrontar as diferentes visões estratégicas e operacionais sobre um mesmo conjunto de perguntas colocadas a todos os entrevistados.

Deste modo, a ideia central passa por identificar pontos de convergência e de divergência entre essas perspetivas e, em seguida, comparar essas posições com a base teórica já existente sobre inteligência policial, gestão do risco e segurança pessoal.

Ao articular estas dimensões pretendemos ir além da mera descrição dos resultados, articulando o conteúdo das entrevistas e a revisão de literatura, identificando as principais lacunas e constrangimentos informacionais que afetam a atividade do CSP e, sobretudo, fundamentar propostas concretas de melhoria que contribuam para potenciar a integração de inteligência policial na segurança pessoal.

III. 1. Diagnóstico da Atual Estrutura Informacional

A análise das entrevistas realizadas, incidindo, neste subcapítulo, sobre as primeiras questões relativas à caracterização da realidade atual da atividade de segurança pessoal, permite identificar um conjunto de fragilidades estruturais no modo como a informação é produzida, partilhada e operacionalizada no contexto do CSP. O atual sistema, embora funcional em determinados domínios, apresenta ainda algumas limitações que pretenderemos colmatar com as contribuições do presente trabalho de investigação.

Desde logo, destaca-se uma assimetria na perceção da suficiência informacional, refletida nos diferentes níveis hierárquicos. Enquanto alguns entrevistados com funções de âmbito estratégico referem a existência de mecanismos estruturados de suporte informacional, assentes numa "ampla variedade de fontes seguras e confiáveis […] que resultam de produção informacional própria/interna e/ou tramitam pelo SINTEL/PSP e/ou pela Plataforma Partilhada de Operações de Segurança do SSI (PPOS)" (E2, 2026). Outros elementos com experiência operacional direta descrevem uma realidade onde existem lacunas significativas no acesso à informação, como refere E5 (2026), "na maior parte das vezes […] não é transmitida qualquer informação sobre o porquê de aquela pessoa necessitar de segurança", sendo frequentemente necessário recorrer a pesquisas autónomas. Esta perceção é corroborada pelo E7 (2026), ao afirmar que "não sabemos tanto quanto gostaríamos e quanto deveríamos saber", evidenciando um défice informacional no plano operacional e tático.

Paralelamente, emerge como uma das principais fragilidades a insuficiente sistematização do fluxo informacional, tanto no plano vertical como horizontal. Embora seja reconhecida a necessidade de um modelo assente na recolha contínua e análise permanente, sendo referido que "tem que haver sempre um mecanismo permanente de recolha e tratamento de informação que permita antecipar cenários" (E1, 2026), a sua concretização prática revela-se desigual. Na realidade operacional, a recolha de informação tende a depender da iniciativa individual, não existindo orientações uniformes ou procedimentos padronizados. Como sublinha E4 (2026), "não temos mecanismos padronizados […] cada um acaba por fazer aquilo que entende como mais importante", sendo esta lógica igualmente reconhecida ao nível do terreno, onde "parte muito da iniciativa de cada um, quando não devia ser assim" (E5, 2026). Ainda que alguns entrevistados refiram a existência de formação inicial nesta matéria, nomeadamente através de módulos ministrados pelo DIP (E7, 2026), a sua aplicação prática não assume um carácter sistemático nem uniforme.

A esta limitação acresce, em alguns contextos, uma insuficiente articulação entre as estruturas de inteligência e o CSP. Esta realidade conduz frequentemente a uma tendência reativa, em que a partilha de informação ocorre sobretudo em situações de maior criticidade ou visibilidade. Como referido, "em situações normais de visitas, isso não acontece […] a não ser que exista algum caso excecional" (E7, 2026). Também o E5 (2026) descreve que "na maior parte das vezes, tirando grandes visitas, praticamente não há informação sobre as ameaças que possam recair sobre a pessoa". Ainda assim, quando essa articulação existe, tende a ser eficaz, o que reforça a ideia de que o problema não reside na inexistência de capacidade, mas na ausência de integração em situações operacionais mais rotineiras.

Neste sentido, assume particular importância a questão da perceção da relevância da informação. Conforme referido pelo E1 (2026) "há uma tendência natural, para poder haver falhas na transmissão de informação, ou transmissão incompleta de informação […] há muita tendência para entrar na lógica da reserva da informação, no princípio da necessidade de conhecer, etc", não apenas por razões de reserva, mas também por uma insuficiente compreensão do valor operacional de determinados dados. Esta limitação é reforçada quando existe uma articulação entre CSP e outras subunidades ou entidades, sendo referido que "acabam por não partilhar alguma informação que viemos a perceber na altura que tinha sido crucial para nós e para a boa execução do serviço" (E6, 2026). Assim, esta dificuldade em equilibrar a reserva da informação com a sua utilização operacional torna este fluxo informacional menos eficiente do que o desejável por quem está no terreno.

No que respeita à oportunidade da informação, os entrevistados reconhecem que, em contextos de maior risco ou complexidade, a informação tende a ser disponibilizada de forma mais estruturada e com maior antecedência. Como refere o E6 (2026), quando o grau de ameaça é mais elevado, "já há um briefing" com informação relevante difundida através dos canais próprios. No entanto, "em situações normais de visitas, isso não acontece […] a não ser que exista algum caso excecional" (E7, 2026), o que evidencia que em situações menos mediáticas ou com menor grau de ameaça, foram identificadas algumas limitações ao nível do tempo de processamento e difusão, que podem afetar a sua utilidade operacional. Ainda assim, alguns entrevistados destacam que, mesmo quando a informação não chega de forma formal e atempada, existem mecanismos operacionais que procuram colmatar essa limitação, nomeadamente através do trabalho das equipas avançadas e da recolha direta de informação no terreno (E1, 2026; E6, 2026), o que permite, em certa medida, compensar as lacunas no fluxo informacional.

Ao nível da formação e capacitação, verifica-se que existem orientações institucionais relacionadas com a recolha de informação, nomeadamente no âmbito da formação inicial e de ações específicas promovidas por estruturas como o DIP. Contudo, os dados sugerem que esta componente não assume ainda um carácter uniforme e transversal a todos os polícias do CSP, sendo frequentemente complementada pela experiência adquirida no terreno. Como refere o E3 (2026), "os polícias do CSP não estão formados, *a priori*, para isto", sendo igualmente apontado que "No que diz respeito à informação, não há uma atenção especial sobre essa matéria" na formação (E4, 2026). Ainda assim, alguns entrevistados referem a existência de orientações e práticas que incentivam a recolha de informação, "somos orientados para esse tipo de recolha e alertados para aquilo que devemos fazer em fontes abertas" (E7, 2026), o que demonstra uma base existente, ainda que não plenamente estruturada.

Em síntese, os dados recolhidos indicam que o sistema informacional do CSP apresenta mecanismos funcionais, sobretudo em contextos de maior exigência. No entanto, persistem limitações ao nível da coordenação, da oportunidade da informação, da sistematização de procedimentos e da capacitação dos polícias, que afetam a consistência do fluxo informacional no quotidiano operacional.

Neste sentido, torna-se pertinente analisar, no subcapítulo seguinte, de que forma os contributos dos entrevistados e a revisão da literatura podem apontar soluções que reforcem a integração da inteligência policial na atividade do CSP.

III. 2. Diagnóstico da Estrutura Informacional Ideal

Analisando agora as respostas dos entrevistados às questões relativas ao reforço da inteligência policial no contexto do CSP, estas permitem identificar um conjunto de dimensões que apontam para a necessidade de uma maior integração entre a produção de informações e a atividade operacional. Estes contributos, quando articulados com o enquadramento teórico anteriormente desenvolvido, permitem consolidar a ideia de que a inteligência policial, no contexto da segurança pessoal, deve ser entendida como uma função orientada para a ação, para a redução da incerteza e para a antecipação do risco (Fernandes, 2014; Elias, 2022).

Em primeira medida destacamos a necessidade de existir proximidade funcional entre a vertente das informações e o âmbito operacional. Uma parte dos entrevistados sublinha que a utilidade da informação depende diretamente da sua ligação às necessidades concretas das equipas no terreno. Neste sentido, é defendida, tanto ao nível estratégico como operacional, a existência de uma componente de inteligência dedicada ou diretamente articulada com o CSP. Como refere o E1 (2026), "Tem que existir, dentro do CSP, uma unidade ou uma capacidade de produção de *intelligence* que consiga, desde logo, recolher informação, ou, pelo menos, receber informação das várias fontes". Neste sentido, também o E7 (2026) destaca que deveria esta componente de inteligência estar inserida "diretamente na estrutura da segurança pessoal, o que até poderia fazer mais sentido, por haver maior sensibilidade para a realidade operacional". Relativamente aos contributos de quem está no terreno, o E6 (2026) aponta para a necessidade de "equipas de informação só a trabalhar para o CSP". De forma convergente, o E7 (2026) refere que "há necessidade de a inteligência policial estar diretamente a trabalhar connosco na parte operacional, integrada mesmo nas equipas, porque nós precisamos de informação em tempo útil".

Esta perceção empírica reforça o que já havia sido sustentado na literatura, nomeadamente no âmbito do policiamento orientado pelas informações, onde se defende que a *intelligence* só produz valor quando integrada no processo decisório e próxima da ação (Ratcliffe, 2008). Também Elias (2022) sublinha que a afirmação das Ciências Policiais passa pela capacidade de transformar conhecimento em ação, o que pressupõe também uma articulação efetiva entre análise e operação. Assim sendo, os dados apontam para uma limitação já identificada no subcapítulo anterior, a existência de capacidade informacional, mas com uma integração ainda incompleta no plano operacional.

Um segundo eixo relevante prende-se com a necessidade de produção de informação contextualizada e orientada para o risco específico de cada missão. Os entrevistados convergem

na ideia de que a mera identificação da ameaça é insuficiente, sendo necessário desenvolver análises dinâmicas e ajustadas ao contexto operacional. Como refere o E4 (2026), devem "produzir avaliações de risco dinâmicas, por evento e por deslocação. Ou seja, não termos algo muito macro e geral, mas algo mais pormenorizado e ajustado a cada serviço", considerando o perfil da entidade protegida, o ambiente e as circunstâncias específicas da missão. Esta necessidade de adaptação ao contexto operacional é ainda coerente com os contributos que destacam a importância da recolha contínua de informação e da antecipação de cenários (E1, 2026), evidenciando que a informação relevante deve resultar de uma leitura dinâmica do ambiente. Este entendimento encontra respaldo direto na literatura sobre gestão do risco, onde se defende que o risco resulta da interação entre ameaça, vulnerabilidade e impacto (Torres, 2015), não podendo ser analisado de forma isolada ou estática.

Um terceiro eixo que identificamos diz respeito à questão da prevenção e da antecipação. Neste sentido, vários entrevistados destacam a importância de atuar antes da materialização da ameaça, através da recolha de informação, da análise do ambiente e da adaptação do dispositivo. Como refere o E7 (2026), a segurança pessoal "deve trabalhar, sobretudo na prevenção", enquanto o E1 (2026) aponta para a necessidade de recolha de informação no terreno antes da chegada da entidade. Também o E2 (2026) destaca o desenvolvimento de medidas de (contra)inteligência, com enfoque na deteção precoce de ameaças. Esta perspetiva articula-se com o modelo de atuação preventiva já abordado no capítulo anterior, nomeadamente com a lógica da redução da incerteza e da antecipação de cenários (Fernandes, 2014; Torres, 2018).

Um quarto eixo prende-se com um especial enfoque na valorização das fontes abertas e da proteção em ambiente digital. Os entrevistados referem consistentemente a necessidade de monitorizar redes sociais, e uma crescente preocupação em questões de cibersegurança. Como refere o E4 (2026), "Ter alguém dedicado a pesquisar nessas fontes, a perceber se existe algum movimento, ainda que pequeno, contra os ideais ou contra a figura da pessoa que estás a proteger, seria extremamente útil". Enquanto o E7 (2026) destaca que "Neste momento, uma das maiores ameaças com que nos deparamos é a cibersegurança. Temos de evoluir nessa área.". Também o E2 (2026) sublinha a necessidade de "sustentação de contramedidas, operacionais e/ou de (contra)inteligência policial, em especial o desenvolvimento de ações de contravigilância e a monitorização de ciber e tecnoameaças, são essenciais/prioritárias para o CSP". Tal como foi abordado anteriormente, as fontes abertas constituem hoje um complemento essencial às fontes tradicionais, permitindo uma leitura mais ampla do contexto

operacional. Neste sentido, os dados empíricos reforçam a necessidade de integrar de forma sistemática esta dimensão na atividade operacional do CSP.

Por último, relativamente à forma como a informação circula entre quem produz inteligência policial e quem comanda ou executa operações de segurança pessoal, os entrevistados convergem na ideia de que a principal limitação não está na produção de informação, mas na forma como esta circula entre quem a produz e quem a utiliza na segurança pessoal. Desde logo, é destacada a necessidade de garantir um fluxo de informação contínuo e eficaz. Como refere o E1 (2026), "tem que existir um fluxo de informação contínuo", sublinhando que essa circulação depende de uma "perceção real do que podem ser vetores de ameaça". Esta ideia evidencia que a eficácia da informação não depende apenas da sua existência, mas da sua relevância e compreensão no contexto operacional.

Por outro lado, concluímos que deve haver uma preocupação de evitar a dispersão da informação, como refere o E3 (2026), "a informação tem que ser centralizada", alertando que a separação entre quem trabalha a informação e quem executa a operação conduz à "dispersão". Neste sentido, é igualmente referida a importância de formalizar os canais de partilha de informação. O E4 (2026) propõe a criação de "um canal formal e obrigatório de partilha prévia de informação", evidenciando a necessidade de tornar este processo mais estruturado e regular.

Paralelamente, destacamos também o papel da tecnologia na melhoria da circulação da informação, sendo que E2 (2026) aponta para uma carência, sobretudo, ao nível do investimento tecnológico. No entanto, esta questão acabaria por ser benéfica no sentido em que como sugere o E4 (2026) "Outra medida importante seria a criação de uma plataforma tecnológica segura e acessível em tempo real para atualização do risco", suportado pelo E7 (2026) quanto à possibilidade de criar uma plataforma digital com acesso rápido à informação, sem comprometer a segurança da informação.

Importa ainda referir que, apesar da relevância da contrainteligência, os entrevistados não valorizam significativamente a utilização de estratégias ativas de desinformação no contexto da segurança pessoal. Pelo contrário e, como demonstrado anteriormente no subcapítulo da contrainteligência e desinformação na segurança pessoal, os dados apontam para uma maior ênfase na prevenção de fugas de informação e na gestão da exposição de medidas operacionais.

III.3. Propostas de Otimização do Sistema de Inteligência Policial

A análise desenvolvida ao longo dos capítulos anteriores permitiu clarificar que a atividade de segurança pessoal, no contexto do CSP, se encontra inserida num ambiente

dinâmico marcado por elevada complexidade e incerteza, exigindo, por isso, modelos de atuação que privilegiem tanto a antecipação como a proatividade na reação. Tal como sublinhado por Fernandes (2014), "inteligência policial […] tem como objetivo essencial reduzir a incerteza inerente à decisão policial e promover abordagens proactivas aos problemas de criminalidade […] (atuais e emergentes), bem como contribuir para o sucesso das operações policiais" (p.165). Contudo, os resultados empíricos demonstraram que, apesar da existência de produção de informação relevante, persistem fragilidades significativas na sua integração na componente operacional.

Os contributos empíricos recolhidos evidenciam que a informação nem sempre chega de forma estruturada ao terreno, nem é devidamente devolvida ao sistema após a sua recolha. Como refere E1 (2026), a capacidade de antecipação depende de um "mecanismo permanente de recolha e tratamento de informação" que permita adaptar continuamente a operação. No entanto, essa lógica de ciclo contínuo, que a doutrina identifica como fundamental no processo de produção de inteligência policial, não se encontra plenamente consolidada, verificando-se disfunções ao nível da circulação e partilha da informação. Esta realidade é coincidente com o que Elias (2022) identifica como um dos desafios centrais das Ciências Policiais, a necessidade de uma efetiva articulação entre conhecimento científico, inteligência e prática operacional, numa lógica integrada e multidisciplinar.

É neste enquadramento que emergem as propostas do presente estudo, não como soluções isoladas, mas como uma resposta estruturada às lacunas identificadas, visando reforçar a integração da inteligência policial numa cultura informacional com reflexo na atividade operacional do CSP.

Ao nível organizacional, a proposta de criação de uma componente de inteligência policial no seio do CSP encontra fundamento direto na necessidade, evidenciada ao longo da investigação, de assegurar um fluxo contínuo e estruturado de informação. Neste sentido, e com base nos contributos empíricos, esta são as prioridades operacionais e táticas que propomos e que esta componente de inteligência deve contemplar:

1. **Capacidade própria, contínua e centralizada de informações.** Os entrevistados convergem na necessidade de o CSP dispor de uma estrutura dedicada à recolha, tratamento e difusão de informação. E1 (2026) refere que deve existir uma capacidade que "receba informação das várias fontes" e a "processe e difunda internamente". Esta prioridade traduz-se na criação de um ciclo contínuo e autónomo de inteligência policial, evitando uma dependência excessiva de outras estruturas e garantindo apoio em tempo útil à operação.

2. **Produção de avaliações do risco dinâmicas e ajustadas à missão.** Devem ser produzidas avaliações do risco específicas para cada deslocação, evento e entidade protegida. O E4 (2026) destaca que estas avaliações devem ser "dinâmicas" e integrar variáveis como o perfil da entidade, o contexto político-social e o comportamento da população.

3. **Foco na antecipação e prevenção da ameaça.** A prioridade central da inteligência policial no CSP deve assumir um carácter preventivo. O E7 (2026) afirma que "o mais importante é a prevenção", sendo igualmente referido por E1 (2026) a necessidade de identificar ameaças com antecedência suficiente para permitir a sua neutralização.

4. **Recolha ativa de informação no terreno através de equipas avançadas.** Considerando o contexto de incerteza e imprevisibilidade anteriormente abordado por Torres (2018), o CSP deverá dispor da capacidade de projetar antecipadamente equipas especializadas na recolha de informações (e, se possível, também capacitadas para intervenção) no terreno, para identificar de vulnerabilidades que permitam ajustar o dispositivo policial.

5. **Apoio direto à decisão e autonomia no terreno.** Devido ao contexto dinâmico em que o CSP opera, E1 (2026) destaca que os elementos no terreno devem dispor de autonomia para alterar itinerários ou procedimentos com base na informação disponível, sem dependência permanente do comando. Isto reforça a necessidade de uma inteligência que não seja apenas informativa, mas que suporte também responsabilidade e decisões de cariz operacional em tempo real.

6. **Monitorização de fontes abertas e ciberameaças.** Os entrevistados evidenciam a crescente importância da dimensão digital. E4 (2026) e E7 (2026) destacam a monitorização de redes sociais, notícias e discursos online como forma de identificação de hostilidades ou potenciais ameaças. Estes contributos são coincidentes ao que fora abordado no âmbito das OSINT, sendo uma prioridade que a inteligência policial se adapte neste sentido.

Ao nível formal e material o investimento na formação neste tipo de matérias deve ser uma condição essencial para a operacionalização eficaz da inteligência policial no CSP. Tal como evidenciado ao longo da revisão teórica, a interpretação da informação depende, em larga medida, das competências dos atores envolvidos, sendo a dimensão humana um fator crítico na qualidade do produto informacional.

No plano procedimental, as propostas apresentadas visam traduzir, em termos concretos, os princípios teóricos anteriormente discutidos, nomeadamente ao nível da antecipação, da adaptação e da integração da informação.

A reativação das ERTE constitui, neste contexto, uma das principais propostas, pois como já fora referido, concretizam de forma evidente um modelo híbrido que articula a vertente informacional com a operacional. Tal permite não apenas a recolha de Informação em contexto real, mas também a intervenção imediata perante ameaças emergentes. Como referido por E1 (2026), a análise do ambiente não pode ser pontual, devendo ser realizada de forma permanente e antecipada, através de equipas dedicadas que permitam compreender o contexto em que a operação se desenvolve. Esta abordagem está também em linha com o modelo de POI, onde a recolha de informação no terreno assume um papel fundamental na construção do conhecimento.

Também a integração do modelo DIDRA reforça esta lógica, permitindo estruturar o processo de decisão e reduzir a dependência de outras abordagens menos estruturadas. Tal como discutido anteriormente, a necessidade de sistematização dos processos de avaliação de risco constitui uma das lacunas identificadas, sendo o DIDRA uma ferramenta que permite colmatar essa fragilidade, promovendo uma abordagem mais racional e consolidada.

No que concerne à contravigilância, a proposta da sua inclusão como procedimento estruturado no seio do CSP, decorre diretamente da análise desenvolvida no capítulo anterior. O E3 (2026) refere que "entendo a contravigilância como uma projeção operacional da contrainteligência", ou seja, se a contrainteligência visa identificar e neutralizar ameaças informacionais, a contravigilância constitui a sua expressão operacional no terreno, permitindo detetar ações hostis de recolha de informação. A sua aplicação responde assim à necessidade, evidenciada empiricamente, de reforçar a capacidade de antecipação e de deteção precoce de ameaças, reduzindo também a dependência de uma atuação meramente reativa.

De igual modo, a vertente da Segurança Eletrónica surge como uma extensão natural desta abordagem, integrando a dimensão tecnológica da contrainteligência. A sua utilização, já consolidada no apoio ao CSP através do DIP, permite detetar ameaças técnicas que não são percetíveis através da observação direta de um espaço onde a entidade estará presente, por exemplo.

Neste sentido, as ações de desinformação e a contenção da exposição informacional, particularmente no domínio digital, articulam-se igualmente com a lógica de contrainteligência anteriormente analisada. Tal como discutido com base em Rid (2021), a gestão do ambiente informacional constitui um elemento central na mitigação de ameaças, sendo a redução da previsibilidade um fator crítico na proteção de entidades.

Em síntese, as propostas apresentadas resultam de uma articulação direta entre o enquadramento teórico desenvolvido e os dados empíricos recolhidos, procurando responder de forma prática e objetiva às lacunas identificadas. Mais do que introduzir novos elementos, visam consolidar e integrar práticas já existentes, conferindo-lhes coerência e base teórica, e tornando o modelo de inteligência policial no CSP verdadeiramente orientado pelas informações.

III.4. Sugestão de Aplicação Prática

Não obstante as propostas anteriormente apresentadas, a principal conclusão que emerge da presente investigação não reside apenas na identificação de lacunas operacionais ou estruturais, mas, principalmente, na existência de uma cultura organizacional predominantemente operacional, em detrimento de uma verdadeira cultura de informações. Esta realidade traduz-se na ausência de uma vertente integrada de *intelligence*, quer numa perspetiva *top-down* quer numa lógica *bottom-up*[25], como fora demonstrado através dos contributos empíricos recolhidos.

Desta forma, como foi possível constatar ao longo da análise, a informação existe, circula e é, em determinados momentos, utilizada, mas não constitui ainda o elemento basilar da atividade de segurança pessoal. Reforça-se novamente o que fora referido por E1 (2026), em que a antecipação depende de um "mecanismo permanente de recolha e tratamento de informação", o que pressupõe não apenas a existência de informação, mas a sua integração num ciclo contínuo e bem estruturado. Contudo, este ciclo ainda não se encontra plenamente consolidado, sendo frequentemente suprido pela capacidade de adaptação e iniciativa dos polícias no terreno, o que, embora revele profissionalismo e experiência, não constitui uma solução viável nem desejável a longo prazo.

Assim sendo, torna-se evidente que a transformação do modelo atual não poderá ser alcançada apenas através de medidas de sensibilização ou ajustes incrementais, exigindo-se uma mudança efetiva de cultura organizacional, onde a informação seja assumida como recurso central e transversal à atividade operacional. Tal mudança implica, necessariamente, a formalização de procedimentos e a criação de mecanismos que garantam a sua aplicação de forma consistente.

[25] *Top-down* refere-se a uma abordagem descendente, em que a produção e orientação dos fluxos informacionais partem dos níveis estratégicos para os operacionais, enquanto *bottom-up* designa uma abordagem ascendente, assente na recolha de informação no terreno e na sua subsequente integração nos níveis superiores de decisão, refletindo diferentes dinâmicas de circulação do conhecimento no seio das organizações (Lowenthal, 2022).

Esta ausência de formalização de procedimentos, não só contribui para a heterogeneidade das práticas, como fragiliza também a própria responsabilização institucional, na medida em que, não havendo "nada escrito" e bem definido, se perde consistência na avaliação das decisões quando ocorrem falhas.

Deste modo, propõe-se, com base neste trabalho de investigação e noutros de especial relevância, um modelo de atuação baseado em procedimentos mandatórios associados a um determinado nível de risco, à semelhança do que já existe relativamente aos graus de ameaça no PCCCFSS, mas adaptado ao contexto específico da segurança pessoal.

A título de exemplo, sugere-se a definição de três níveis de risco no contexto da segurança pessoal (moderado, elevado e crítico), partindo do pressuposto de que a própria existência de segurança pessoal já indicia a presença de ameaça relevante e de vulnerabilidades significativas, não se justificando a consideração de níveis inferiores.

Para cada um destes níveis, deverão ser definidos conjuntos diferenciados de procedimentos, como se identifica na figura 7, que se apresenta de seguida:

Figura 7

Quadro Exemplo de Procedimentos consoante Níveis de Risco

N.º	**Identificação nível Risco:**	**Procedimentos:**
1	Crítico	Aplicação obrigatória de todas as medidas estruturantes, incluindo: • Ativação de ERTE; • Implementação de ações de contravigilância através de equipas especializadas (UEP/CSP); • Limpeza eletrónica dos espaços sensíveis através de uma equipa especializada em Segurança Eletrónica; • Construção prévia de cenários e subcenários no auxílio ao planeamento; • Briefing prévio sobre o contexto do perfil da pessoa protegida, do local e as circunstâncias específicas da missão; • Monitorização contínua de fontes abertas e ambiente digital;
2	Elevado	Aplicação de um conjunto de medidas, ainda que com maior flexibilidade, podendo ser ajustadas em função do contexto operacional, mantendo, contudo, a obrigatoriedade de determinados procedimentos, como: • Equipa de Segurança Avançada no terreno para recolha de informação; • Construção prévia de cenários e subcenários no auxílio ao planeamento; • Briefing prévio sobre o contexto do perfil da pessoa protegida, do local e as circunstâncias específicas da missão; • Monitorização contínua de fontes abertas e ambiente digital;
3	Moderado	Maior flexibilidade e autonomia dos operacionais no terreno para a tomada de decisão. Mantendo as medidas obrigatórias de: • Construção prévia de cenários e subcenários no auxílio ao planeamento; • Briefing prévio sobre o contexto do perfil da pessoa protegida, do local e as circunstâncias específicas da missão; • Monitorização contínua de fontes abertas e ambiente digital;

Nota: Elaboração Própria

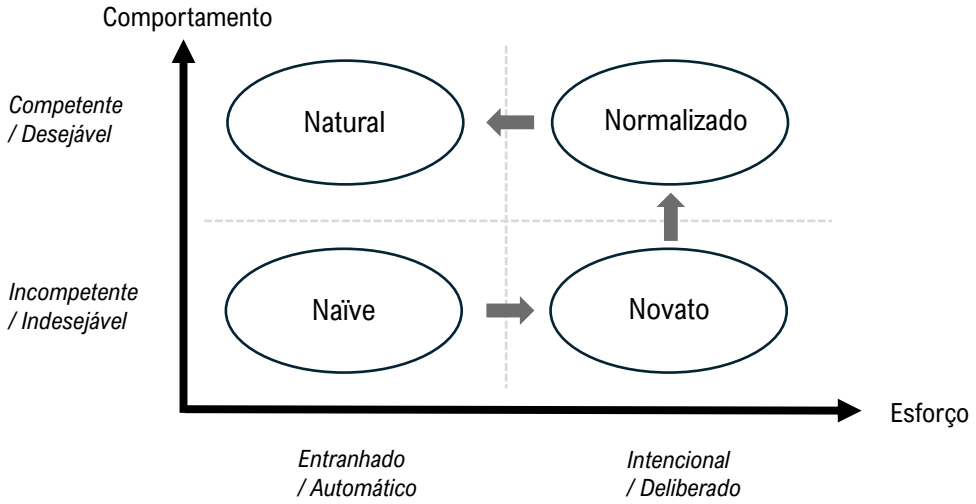
Este modelo permite, por um lado, assegurar uma resposta proporcional ao nível de risco e, por outro, conferir também maior autonomia e eficiência operacional, evitando soluções desajustadas ao contexto em que se está a atuar.

Importa sublinhar que esta proposta não visa substituir o julgamento profissional dos operacionais, mas antes fornecer um quadro de referência bem consolidado que oriente a tomada de decisão, reduzindo assim a dependência de abordagens exclusivamente intuitivas. Tal como evidenciado ao longo da investigação, a ausência de sistematização constitui uma das principais fragilidades do modelo atual, sendo a formalização de procedimentos algo que consideramos essencial existir.

E num raciocínio semelhante, propõe-se ainda, como linha de investigação futura, o desenvolvimento de um estudo ainda mais aprofundado nesta matéria que permita a criação de uma eventual NEP dedicada à vertente da inteligência policial no CSP. Ou até, a elaboração de manuais doutrinários específicos, que sistematizem práticas, conceitos e procedimentos no domínio da segurança pessoal.

Figura 8

Posicionamento face à cultura informacional PSP



Nota: Adaptado de "Fundamentals of risk management: understanding, evaluating and implementing effective risk management", by P. Hopkin, 2017, p. 300.

Em última análise, a transformação proposta assenta na ideia de que a eficácia da segurança pessoal depende, cada vez mais, da capacidade de integrar informação, antecipar e reagir a ameaças, estruturando a ação de forma coerente e sistematizada. À luz da figura 8, de Hopkin (2017), o CSP tende ainda a posicionar-se num nível em que a componente de

informações depende sobretudo de um esforço deliberado e da iniciativa individual dos polícias, aproximando-se dos quadrantes "Naïve" ou "Novato". O objetivo deverá ser, numa primeira fase, evoluir para o quadrante "Normalizado", através da formalização de procedimentos e da integração clara da inteligência policial na vertente operacional e, posteriormente, atingir um patamar "Natural", onde a cultura de informações esteja plenamente enraizada no funcionamento da subunidade. Sem essa mudança de paradigma, de uma cultura operacional articulada com uma verdadeira cultura de informações, qualquer melhoria tenderá a ser pontual e limitada, não respondendo plenamente às exigências do ambiente securitário contemporâneo.

Conforme refere Nassim Taleb (2011), autor que popularizou a teoria do cisne negro, já mencionado anteriormente como sendo eventos raros, imprevisíveis e de impacto extremo que estão fora das expectativas normais, são difíceis de prever, mas parecem óbvios após ocorrerem, levando a narrativas falsas de previsibilidade. Nesse sentido, é fundamental que os Estados e as respetivas instituições, entre as quais, se destacam os serviços de informações e as forças de segurança, desenvolvam metodologias científicas de pesquisa e análise de informações estratégicas e sobretudo operacionais para antecipar ameaças (por vezes, invisíveis, mas omnipresentes), a análise do risco, assim como a proposta de reforço das medidas de segurança e de mitigação de vulnerabilidades.

A revolução tecnológica em curso, particularmente acelerada no início do século XXI, tem trazido para o quotidiano das sociedades hodiernas a utilização de drones, da robótica e da inteligência artificial, os quais, se podem constituir como ameaças, mas também como oportunidades para o reforço dos dispositivos de segurança. Caberá, assim, aos Estados e respetivas FSS apostar cada vez mais nas novas tecnologias, complementando o seu uso com o fator humano e abandonando em grande medida a aposta em mão de obra intensiva nas operações mais complexas e de maior dimensão. A complementaridade e simbiose entre as novas ferramentas tecnológicas, sistemas de informação e a segurança pessoal serão cruciais no futuro.

Conclusão

Tendo chegado ao final do presente estudo, importa agora sintetizar as principais conclusões decorrentes da sua elaboração, bem como responder à pergunta de investigação inicialmente formulada. Ao longo da dissertação, procurou-se analisar de que forma uma componente de inteligência policial, dedicada a apoiar a atividade operacional do Corpo de Segurança Pessoal, poderá potenciar a eficácia das operações de segurança de altas entidades. A investigação permitiu verificar que, num contexto securitário cada vez mais complexo, dinâmico e, sobretudo, marcado por elevados níveis de incerteza, a inteligência policial assume-se como um instrumento decisivo para reduzir a surpresa, aumentar a perceção situacional e apoiar a tomada de decisão operacional, em consonância com a literatura de referência sobre o papel da inteligência no contexto policial, designadamente Fernandes (2014) e Elias (2022).

De acordo com o enquadramento teórico desenvolvido, foi possível compreender que a segurança pessoal, enquanto competência reservada da PSP, não pode ser dissociada da produção e tratamento de informações. Tal como ficou demonstrado nos dois primeiros capítulos, a natureza dos riscos e ameaças associados à proteção de altas entidades exige uma abordagem que vá para além da mera aplicação de medidas físicas de proteção, impondo a existência de uma avaliação contínua do contexto, das vulnerabilidades do protegido e da evolução do ambiente operacional. Neste sentido, a articulação entre a segurança pessoal e a inteligência policial surge como um elemento essencial para uma atuação mais preventiva, proativa e ajustada à realidade concreta, permitindo reforçar a eficácia das equipas no terreno.

Responde-se agora à questão matricial da presente dissertação que se versa sobre como poderá uma componente de inteligência policial, dedicada a apoiar a atividade operacional do CSP, potenciar a eficácia no processo de segurança de altas entidades e outras que beneficiam de segurança pessoal, sendo que a resposta que emerge do presente estudo é a de que tal componente poderá potenciar significativamente a eficácia do CSP se for integrada na estrutura operacional, através da formalização de procedimentos consoante as avaliações de risco dinâmicas. Conclui-se, como proposta de cariz organizacional, que as prioridades operacionais e táticas propostas com base na revisão bibliográfica, análise documental e nos contributos empíricos desta componente de inteligência policial convergem na necessidade de dotar o CSP de uma capacidade própria, contínua e centralizada de informações, capaz de receber, tratar e difundir internamente informação útil em tempo oportuno. A este ponto acrescenta-se a capacidade de produzir avaliações de risco dinâmicas e ajustadas a cada missão, bem como o

reforço da recolha ativa de informação no terreno, designadamente através de equipas avançadas com capacidade de detetar potenciais vulnerabilidades e ajustar o dispositivo operacional no terreno. Em paralelo, evidencia-se a pertinência de consolidar a monitorização de fontes abertas, a vertente tecnológica da contrainteligência e contravigilância, enquanto instrumentos de identificação atempada de vulnerabilidades.

No que se refere à primeira questão derivada de compreender de que forma as lacunas de articulação com outras subunidades e entidades na partilha de inteligência policial podem comprometer a eficácia operacional do CSP, concluiu-se que essas lacunas acabam por reduzir significativamente a fluidez da informação, dificultando a contextualização da ameaça e atrasando uma eventual resposta operacional. A investigação mostrou que, apesar da existência de entidades e estruturas com competência informacional, subsistem fragilidades no modo como a informação é partilhada, consolidada e transformada em conhecimento útil para o CSP. Assim, quando a articulação interinstitucional não é célere nem suficientemente densa e adaptada ao contexto operacional, diminui-se a capacidade de planeamento, de antecipação e de reação, o que pode comprometer a proteção eficaz de altas entidades.

Relativamente à segunda questão derivada sobre em que medida a integração de uma componente de inteligência policial poderá melhorar a perceção situacional e a capacidade de resposta das equipas de segurança pessoal perante ameaças dinâmicas, a investigação permitiu concluir que o seu impacto seria claramente positivo. A disponibilização de informação tratada, atualizada e contextualizada permite às equipas operar com maior consciência situacional, melhorando a leitura do ambiente, a identificação precoce de sinais de risco e a capacidade de adaptação a cenários dinâmicos. Tal como evidenciado pela revisão bibliográfica e reforçado pelos entrevistados, a perceção situacional constitui uma condição indispensável para a segurança pessoal eficaz, sendo potenciada quando existe um sistema de inteligência com capacidade para integrar dados de várias origens, incluindo do terreno, e desta forma auxiliar a tomada de decisão. Neste ponto, autores como Torres (2015) e Fernandes (2014) ajudam a sustentar a ideia de que a incerteza só pode ser gerida de forma consistente quando a decisão é apoiada por inteligência.

No que concerne à terceira questão derivada, relativamente à pertinência de uma atividade própria de contrainteligência e desinformação no seio do sistema informacional do CSP, a investigação permitiu aferir que a dimensão da contrainteligência é particularmente relevante, sobretudo no que respeita à proteção da informação, à salvaguarda dos procedimentos operacionais e à deteção de vulnerabilidades. Neste sentido, a contrainteligência

procura identificar e neutralizar ameaças de natureza informacional, enquanto a contravigilância traduz essa finalidade no plano operacional. A sua aplicação responde, assim, à necessidade empiricamente evidenciada de reforçar a capacidade de antecipação e de deteção precoce de ameaças, reduzindo a dependência de uma atuação meramente reativa. Já no que toca à desinformação, os contributos recolhidos apontam para uma maior prudência na sua formulação como prática autónoma no contexto do CSP, embora a sua lógica possa ser considerada em situações muito específicas com o objetivo de dispersar a atenção que recai sobre a entidade protegida. Conclui-se que, mais do que desenvolver estratégias complexas de desinformação, importa priorizar neste momento o reforço e a organização das práticas já existentes, tornando o modelo mais eficaz e ajustado às atuais exigências.

No capítulo III foram apresentadas propostas de otimização do sistema de inteligência no CSP que importa agora retomar, ainda que de forma sintética. Conclui-se, a nível formal e material, que se deve em primeiro lugar, fazer uma aposta na formação neste tipo de matérias. A autonomia e a sensibilidade na dimensão da inteligência policial está diretamente ligada à qualidade da interpretação da informação e às competências dos atores envolvidos, pelo que a dimensão humana dos operacionais no terreno deve ser tratada como um fator crítico no seu desempenho. Em termos procedimentais, impõe-se a criação de um modelo de atuação que privilegie a antecipação, ao invés de uma lógica meramente reativa. Neste sentido, entre as medidas mais relevantes, destaca-se a ativação das ERTE (Equipas de Reação Tática Encoberta), que enquanto instrumento tático, materializam um modelo híbrido entre informações e operações, permitindo não só recolher dados no terreno, mas também reagir de forma imediata sobre ameaças emergentes. Dado o novo contexto de imprevisibilidade e conforme Torres (2020), a imprevisibilidade da ameaça deve corresponder a uma resposta igualmente flexível, sendo que as ERTE favorecem uma abordagem adaptativa, essencial à gestão da incerteza. A esta proposta associa-se ainda o reforço da contravigilância, entendida como expressão prática da contrainteligência no terreno, permitindo detetar ações hostis de recolha de informação e reduzir a vulnerabilidade do dispositivo no terreno. A sua aplicação, responde assim à necessidade evidenciada empiricamente de privilegiar a antecipação e não depender de uma atuação meramente reativa.

Em termos práticos, propõe-se ainda, como linha de investigação futura, a adoção de um modelo de procedimentos mandatórios consoante o grau de ameaça e o nível de risco associados à entidade protegida, bem como a formalização de medidas padronizadas através de uma NEP inteligência policial e análise do risco no CSP. O objetivo destas medidas seria

promover uma mudança efetiva de cultura organizacional para uma cultura de informações, garantindo também a uniformidade das práticas, a responsabilização institucional e a atuação do CSP com uma lógica mais proativa, sistemática e adaptada ao atual contexto criminal. A missão policial e, em concreto, a segurança pessoal não deve ser casuística e baseada em elementos essencialmente empíricos.

Não obstante os contributos alcançados, é essencial reconhecer também as limitações inerentes à investigação. A natureza sensível e reservada do tema levou à codificação dos entrevistados, o que, embora necessário para proteger fontes, limitou a profundidade de identificação e análise. Optou-se pela escolha de perguntas abertas com o objetivo de gerar respostas diversificadas e ricas em propostas, permitindo densificar o trabalho e identificar lacunas, mas inviabilizou a possibilidade de recorrer a uma análise de conteúdo das entrevistas formalizada, dada a especificidade da informação e a escassez de doutrina nacional, que complicaria a articulação entre contributos empíricos e referências teóricas.

No que concerne à amostra, o plano inicial previa quatro oficiais e quatro chefes para equilibrar visões estratégicas e operacionais/táticas, tanto na especialidade do CSP como das informações, no entanto apenas foi possível entrevistar dois polícias com experiência direta em informações na PSP. Esta assimetria reduziu a profundidade na vertente de inteligência policial face à operacionalidade no CSP, limitando a capacidade de equalizar os contributos entre estes domínios. Adicionalmente, restrições no acesso a informação reservada ou confidencial, dado o objeto de estudo do trabalho, obrigaram a uma abordagem mais abstrata em certos tópicos e propostas, recorrendo a bibliografia internacional e analogias com algumas práticas nacionais já existentes. Áreas como gestão de risco, grau de incerteza, cenarização, contrainteligência e desinformação carecem ainda de doutrina consolidada em Portugal, realçando-se também a necessidade de investigação académica focada nestas matérias, face ao ambiente securitário cada vez mais volátil.

Dada a natureza exploratória do estudo, emergem oportunidades para linhas de investigação complementares. Fica por explorar a extensão de uma componente de inteligência policial a outras subunidades da UEP, assim como poderia o núcleo de inteligência policial da UEP adaptar-se às necessidades específicas do CSP e de outras subunidades operacionais. Metodologicamente, alinha-se com as limitações identificadas um estudo qualitativo de maior escala, aproveitando a base teórica aqui construída para uma amostra mais ampla. Isso permitiria priorizar propostas e hierarquizar procedimentos na integração de inteligência no CSP, superando a divergência de respostas e a assimetria da amostra atual. Ainda assim, estas

limitações não comprometem a relevância dos resultados obtidos, sugerem sim a necessidade de aprofundar o tema em estudos futuros, recorrendo a amostras mais alargadas.

Importa, por último, reconhecer que tanto o CSP como a PSP têm demonstrado elevados níveis de eficácia no plano operacional, assegurando, de forma consistente, a segurança e proteção das mais altas entidades em território nacional e internacional. Ainda assim, essa eficácia não deve conduzir a uma excessiva confiança no modelo atual. Como alerta Torres (2018), existe por vezes a perceção de que "nada de relevante […] irá de facto ocorrer no futuro. Uma espécie de *wishful thinking*" (p.18), o que acaba por comprometer a consolidação de uma cultura verdadeiramente orientada pelas informações, cada vez mais necessária num contexto marcado pela incerteza e pela complexidade das ameaças.

Referências Bibliográficas

Abreu, M. (2015). *Formação De Especialização na PSP: Conteúdos Complementares por Classes no curso de Segurança Pessoal* [Relatório Final do I Curso de Comando e Direção Policial, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos de Acesso Aberto de Portugal. https://comum.rcaap.pt/bitstreams/83ba18bf-2ee4-4ded-8ab68a01a4b771e1/download

Araújo, A. C. da S. (2019). *O policiamento e as informações na divisão policial de Sintra: Entre a realidade e a utopia* [Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/30330

Bispo, A. J. (2004). A Função de Informar. Em *Informações e segurança: Estudos em honra do General Pedro Cardoso*. Prefácio.

Bonilla, D. N. (2004). El ciclo de Inteligencia y sus límites. *48*, 51–66.

Campenhoudt, L. V., Quivy, R., & Marquet, J. (2017). *Manual de Investigação em Ciências Sociais* (Edição Portuguesa). Grandiva.

Carrilho, L. (2007). Proteção de Testemunhas—O Papel do CSP. Em *Estudos de Homenagem ao Juíz Conselheiro António da Costa Neves Ribeiro*. Coimbra: Almedina.

Carter, D. (1990). *Law enforcement intelligence: A guide for state, local, and tribal law enforcement agencies* (2nd Edition). Michigan State University.

Carter, D. L., & Carter, J. G. (2009). Intelligence-Led Policing: Conceptual and Functional Considerations for Public Policy. *Criminal Justice Policy Review*, *20*(3), 310–325. https://doi.org/10.1177/0887403408327381

Carvalho, J. (2016). *A geração de cenários no planeamento de operações policiais – uma reflexão metodológica* [Relatório Final – 2º Curso de Comando e Direção Policial, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos

de Acesso Aberto de Portugal. https://comum.rcaap.pt/bitstreams/c93e6fb9-ed58-4bcc-802f-b7fa17ab3475/download

Carvalho, J. B. (2009). Intelligence-Led Policing em Bairros Problemáticos. Em *Estudos de Intelligence* (pp. 111–133). ISCSP. Academia.edu.

Clemente, P. (2009). *As Informações de Polícia*. ISCPSI.

Cope, N. (2004). Intelligence Led Policing or Policing Led Intelligence?: Integrating Volume Crime Analysis into Policing. *British Journal of Criminology*, *44*. ResearchGate. https://doi.org/10.1093/bjc/44.2.188

Corrêa, H. da S. (2018). *Inteligência de segurança pública: O perfil profissional e suas competências* [Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/25252

Couto, A. C. (1988). *Elementos de Estratégia Militar—Apontamentos para um curso: Vol. I.* Instituto de Altos Estudos Militares. https://pt.scribd.com/document/223629047/Elementos-de-Estrategia

Durkheim, É. (2010). *As Regras do Método Sociológico* (11.ª). Barcarena: Editorial Presença.

Ehrman, J. (2009). What Are We Talking About Now, When We Talk About Counterintelligence? *Studies in Intelligence*, *Vol. 68*.

Elias, L. (2022). *Ciências Policiais e Segurança Interna: Desafios e prospetivas*. ISCPSI/ICPOL. Repositórios Científicos de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/51682

Elias, L. (2023). Policing in a Digital Age: Balance between community-based strategies and technological intelligence. *Preparing Law Enforcement for the Digital Age - Special Conference Edition Nr. 6*, 27–37.

Elias, L. M. A. (2022). *Ciências Policiais e Segurança Interna: Desafios e prospetivas* (2ª). ISCPSI/ICPOL. http://hdl.handle.net/10400.26/51682

Escorrega, K. C. F. (2009). A Segurança e os "Novos" Riscos e Ameaças: Perspectivas Várias. *Revista Militar*.

Espírito Santo, P. (2010). *Introdução à metodologia das ciências sociais: Génese, fundamentos e problemas*. Edições Sílabo.

European Comission. (2018). *Tackling online disinformation: A European Approach*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018DC0236

Farinha, L. P. (2007). "O dever de obediência hierárquica". Em *Estudos de Homenagem ao Juiz Conselheiro António da Costa Neves Ribeiro – in memoriam* (pp. 553–568). Coimbra: Almedina.

Felgueiras, S. R. C. (2015). *Ação policial face à ação coletiva: Teoria para uma estratégia de policiamento de multidões* (Lição Inaugural da Abertura Solene do Ano Letivo 2015/2016). ISCPSI. https://www.researchgate.net/publication/316622390_Acao_policial_face_a_acao_coletiva

Fernandes, L. (2004). As sociedades contemporâneas e a ameaça terrorista. *Terrorismo*, 460–481.

Fernandes, L. (2014). *Intelligence e segurança interna*. Instituto Superior de Ciências Policiais e Segurança Interna.

Fernandes, L., & Valente, M. M. G. (2005). *Segurança Interna—Reflexões e Legislação*. Almedina.

Ferreira de Oliveira, J. (2015). *A manutenção da ordem da ordem pública em democracia*. Lisboa: ISCPSI.

Ferreira, T. F. D. S. (2012). *Monitorização de fontes abertas no contexto da investigação criminal: Redes sociais* [Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/32206

Ferreira, V. (2023). *Spotters e inteligência policial: Estudo exploratório no comando distrital de Braga* [Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos de Acesso Aberto de Portugal. https://comum.rcaap.pt/entities/publication/6d4b639e-0224-44cd-a2b8-bff97bae8910

Fortes, A. J. S. (2020). *Informações de segurança versus Informações policiais: Complementaridade ou sobreposição?* http://hdl.handle.net/10400.26/33127

Garcia, T. (2009). *O SEI como plataforma de apoio à análise de informações criminais*.

Giddens, A. (2000). *O Mundo na Era da Globalização*. Lisboa: Editorial Presença.

Goldman, J. (2006). *Words of intelligence: A dictionary*. Scarecrow Press.

Henriques, M., Medeiros, M., Regalado, J., Rosa, J., & Bandeira, L. (2008). *Dossier Regicídio—O Processo Desaparecido*. Lisboa: Tribuna.

Hopkin, P. (2017). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (Fourth edition). Kogan Page.

Hopkin, P. (2018). *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management* (5.ª ed). Kogan Page Publishers.

Júnior, C. M. F. (2008). *A inteligência e a gestão da informação policial*. Fortium.

Lamano, D. (2000). *Executive Protection Specialist*. BTI Press.

Lowenthal, M. (2009). *Intelligence: From Secrets to Policy* (4th ed.). CQ Press.

Lowenthal, M. (2020). *Intelligence: From secrets to policy* (8th ed.). QC Press.

Madeira, J. (2013). *O Atentado a Salazar*. Lisboa: Esfera dos Livros.

Magalhães, C. (2018). *Segurança pessoal e segurança interna*. http://hdl.handle.net/10400.26/34307

Magalhães, C. A. S. (2023). *A Inteligência Policial na Segurança Pessoal de Dignitários: Contributos* [Trabalho Final CCDP, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/45900

Maguire, M., & John, T. (2006). Intelligence Led Policing, Managerialism and Community Engagement: Competing Priorities and the Role of the National Intelligence Model in the UK. *Policing and Society*, *16*(67–85). https://doi.org/10.1080/10439460500399791

Mangio, C. A., & Wilkinson, B. J. (2008). Intelligence Analysis: Once Again. *Air Force Research Laboratory*.

McDowell, D. (2009). *Strategic intelligence: A handbook for practitioners, managers and users*. The Scarecrow Press Inc.

McGovern, C. (2011). *Protective Operations A Handbook for Security and Law Enforcement* (1st Edition). CRC Press.

Medeiros, R. (2001). *Estudo exploratório das informações na PSP* [Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Biblioteca ISCPSI.

Moreira, T. A. C. (2010). *A privacidade dos trabalhadores e as novas tecnologias de informação e comunicação: Contributo para um estudo dos limites do poder de controlo electrónico do empregador* [Dissertação de Doutoramento, Universidade do Minho]. Repositório Universidade do Minho. https://hdl.handle.net/1822/10470

O´Connor, R. (1996). *Bodyguards*. London: Cassel Group Wellinton House.

Oyedokun, T., Adesina, O., Laaro, M., & Ambali, Z. (2022). *Information Versus Intelligence: The Legitimate Approximation and Variability Between Processed Data and Evidence-Based Knowledge*. *0*(18), 51–54. https://doi.org/10.26650/bba.2022.18.1147851

Palmieri, L. (2005). Information Vs. Intelligence: What Police Executives Need to Know. *Police Chief Magazine*. https://www.policechiefmagazine.org/information-vs-intelligence/

Patton, M. Q. (2002). *Qualitative research & evaluation methods* (3rd ed.). Sage.

Pearsall, B. (2010). *Predictive policing: The future of law enforcement?* 16–19.

Pereira, C. (2013). *Análise Criminal e Sistemas de Informação* [Trabalho de Investigação Individual do CEM-C, Instituto de Estudos Superiores Militares]. Repositórios Científicos de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/9973

Peterson, M. (2005). *Intelligence-Led Policing: The New Intelligence Architecture*.

Pherson, R. H., & Heuer, R. J. (2010). *Structured Analytic Techniques for Intelligence Analysis*. CQ Press.

Quivy, R., & Campenhoudt, L. V. (2005). *Manual de investigação em ciências sociais*. Grandiva.

Ramos, R. (2006). *D. Carlos: 1863-1908*. Lisboa: Circulo de Leitores.

Ratcliffe, J. (2003). *Intelligence-led policing*. Australian Institute of Criminology. Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi248

Ratcliffe, J. (2007). *Integrated intelligence and crime analysis: Enhanced information management for law enforcement leaders*. Police Foundation.

Ratcliffe, J. (2008). *INTELLIGENCE-LED POLICING*. Willan Publishing. Academia.edu. https://www.academia.edu/27131667/INTELLIGENCE_LED_POLICING

Redmond, P. J. (2010). The Challenges of Counterintelligence. Em L. K. Johnson (Ed.), *The Oxford Handbook of National Security Intelligence*. Oxford University Press. https://doi.org/10.1093/oxfordhb/9780195375886.003.0033

Rego, P. C. P. (2017). *Terrorismo lone wolf: Uma revisão da literatura* [Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos de Acesso Aberto de Portugal. http://hdl.handle.net/10400.26/19937

Ribeiro, C. (2006). *Combate à criminalidade, prevenção da Ordem Pública e informações policiais* [Curso de Direcção e Estratégica Policial]. ISCPSI.

Rid, T. (2021). *Active measures: The secret history of disinformation and political warfare*. Profile Books.

Rodrigues, I. (2025). *Avaliação do risco em grandes eventos desportivos* [Trabalho Final CCDP, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositórios Científicos de Acesso Aberto de Portugal. https://comum.rcaap.pt/bitstreams/94230cdc-17e7-4dd8-9b30-5c89c7465274/download

Samara, M. A., & Tavares, R. (2008). *O Regícidio*. Lisboa: Tinta-da-china.

Santos, G. M. P. (2020). *Polícia e segurança pessoal* [Dissertação de Mestrado, Faculdade de Direito da Universidade de Lisboa]. Repositórios Científicos de Acesso Aberto de Portugal. http://hdl.handle.net/10451/45811

Schneider, G. (2005). An examination of the required operational skills and training standards for a Close Protection Operative in South Africa. *University of South Africa*.

Shulsky, A. N. (1991). *Silent warfare: Understanding the world of intelligence*. Brassey's.

Taleb, N. N. (2011). *O Cisne Negro — O impacto do altamente improvável*. Dom Quixote.

Telo, A. J. (2011). *Primeira República Vol II - Como Cai um Regime*. Editoral Presença.

Tilley, N. (2005). *Problem-Oriented Policing and Crime Prevention*. Wilian Publishing.

Torres, J. (2011). Segurança "Just ln Time": Abandonar de vez o paradigma da mão-de-obra intensiva – Politeia. *Politeia*, (235–247). https://politeia-online.pt/article/seguranca-just-ln-time-abandonar-de-vez-o-paradigma-da-mao-de-obra-intensiva/

Torres, J. (2015). *Gestão riscos no planeamento, execução e auditoria de segurança*. https://bibliografia.bnportugal.gov.pt/bnp/bnp.exe/registo?1925590

Torres, J. (2018). Terrorismo do Séc. XXI: lidar com o risco ou com a incerteza? *Revista de Segurança e Defesa (38)*, 14–31.

Torres, J. (2020). Uma Polícia para o século XXI: breves reflexões. *Separata Revista de Polícia Portuguesa, V Série*, (2).

Torres, J. (2024). *Manual de Gestão do Risco e da Incerteza*. ISCPSI.

Zedner, L. (2009). *Security (Key Ideas in Criminology)* (1st edition). Routledge.

Legislação

Decreto-Lei n.º 12/2012, de 20 de janeiro. (2012). *Diário da República: I Série, n.º 15/2012*. Presidência do Conselho de Ministros. https://diariodarepublica.pt/dr/detalhe/decreto-lei/12-2012-544382

Decreto-Lei n.º 151/85, de 9 de maio. (1985). *Diário da República: I Série, n.º 106/1985*. Presidência do Conselho de Ministros e Ministérios da Administração Interna e das Finanças e do Plano. https://diariodarepublica.pt/dr/detalhe/decreto-lei/151-1985-152342

Decreto-Lei n.º 321/94, de 29 de dezembro. (1994). *Diário da República: I Série, n.º 300/1994*. Ministério da Administração Interna. https://diariodarepublica.pt/dr/detalhe/decreto-lei/321-1994-322095

Constituição da República Portuguesa. (1976). *Diário da República: I Série, n.º 86/1976, de 10 de abril*. Assembleia da República. https://diariodarepublica.pt/dr/detalhe/decreto-aprovacao-constituicao/502635

Lei n.º 5/99, de 27 de janeiro, Assembleia da República (1999). *Diário da República: I Série* A, nº 22. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=33&tabela=lei_velhas&nversao=3

Lei n.º 7/96, de 29 de fevereiro, da Assembleia da República. (1996). *Diário da República: I Série*, n.º 51/1996. https://diariodarepublica.pt/dr/detalhe/lei/7-621340

Lei n.º 49/2008, de 27 de agosto, da Assembleia da República (Lei de Organização da Investigação Criminal). (2008). *Diário da República: I Série*, 165/2008. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1021&tabela=leis

Lei n.º 53/2007, de 31 de agosto, da Assembleia da República (Lei Orgânica da Polícia de Segurança Pública). (2007). *Diário da República: I Série, n.º 168/2007*. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1079&tabela=leis

Lei n.º 53/2008, de 29 de agosto, da Assembleia da República (Lei de Segurança Interna). (2008). *Diário da República: I Série*, n.º 167/2008. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1012&tabela=leis

Lei n.º 34/2013, de 16 de maio, da Assembleia da República. (2013). *Diário da República: I Série*, n.º 94/2013. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1924&tabela=leis

Lei n.º 4/2014, de 13 de agosto, da Assembleia da República (Lei Quadro do Sistema de Informações da República Portuguesa). (2014). *Diário da República: I Série*, n.º 155/2014. https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?tabela=leis&nid=2204&pagina=1&ficha=1

Portaria n.º 383/2008, de 29 de maio, do Ministérios das Finanças e da Administração Pública e da Administração Interna. (2008). *Diário da República: I Série*, n.º 103/2008. https://diariodarepublica.pt/dr/detalhe/portaria/383-2008-449175

Portaria n.º 379-B/2023, de 17 de novembro, da Presidência do Conselho de Ministros, Administração Interna e Finanças. (2023). *Diário da República: I Série*, n.º 223/2023. https://diariodarepublica.pt/dr/detalhe/portaria/379-b-2023-224462297

Despacho n.º 19935/2008, de 28 de julho, do Ministério da Administração Interna - Direcção Nacional da Polícia de Segurança Pública. (2008). *Diário da República: II Série*, n.º 144/2008. https://diariodarepublica.pt/dr/detalhe/despacho/19935-2008-924735

Despacho n.º 6158/2017, de 13 de julho, da Administração Interna - Polícia de Segurança Pública - Direção Nacional. (2017). *Diário da República: II Série*, n.º 134/2017. https://diariodarepublica.pt/dr/detalhe/despacho/6158-2017-107677747

Regulamentos Internos

Programa de Segurança da Presidência da República. (2021). Presidência da República.

Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança (PCCCOFSS). (2010). Aprovado pela Deliberação n.º 140/2010, de 25 de março, do Conselho de Ministros.

Despacho 3/GDN/2026 - Orgânica da Unidade Especial de Polícia. (2026). Polícia de Segurança Pública.

Diretiva Interna CSP/UEP n.º 02/2012. (2012). Polícia de Segurança Pública.

Ordem de Serviço n.º 25, de 5 de fevereiro (Anexo 2). (2026). Polícia de Segurança Pública.

NEP n.º AUOOS/DIP/02/05, de 30 de dezembro. (2012). Polícia de Segurança Pública.

Apêndices

Apêndice A – Autorizações cedidas pela DN/PSP no âmbito da investigação

A.1. Ofício com pedido de autorização de realização de entrevista n.º 1

MINISTÉRIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS
E SEGURANÇA INTERNA

Exmo. Sr. Diretor Nacional Adjunto, para a UORH,
MI Superintendente-Chefe Ismael Pereira Gaspar Jorge

Assunto: Solicitação de realização de entrevistas no âmbito da dissertação de mestrado

Eu, Rodrigo Miguel Rosa Rodrigues, Aspirante a Oficial de Polícia finalista do Curso de Mestrado em Segurança Pública, no âmbito da realização da dissertação de mestrado intitulada "Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal", sob orientação do(a) Superintendente-Chefe (Doutor) Luís Manuel Elias e coorientação do Superintendente-Chefe José Emanuel de Matos Torres e Intendente Tito Eurico Fernandes, venho mui respeitosamente solicitar a V.ª Ex.ª autorização:

Para a realização das seguintes entrevistas:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

A realização destas entrevistas tem como intuito enriquecer a investigação com contributos críticos e fundamentados com base no conhecimento especializado e experiência operacional dos entrevistados. Deste modo, poderá atingir-se uma base mais sólida de análise sobre a pertinência de criação e operacionalização de uma componente de inteligência policial integrada no Corpo de Segurança Pessoal.

Comprometo-me a manter a confidencialidade dos dados recolhidos, fora do âmbito da elaboração e discussão da dissertação, bem como a cumprir as demais regras éticas relativas à realização de investigação científica.

Pede deferimento.

A.2. Despacho de autorização para realização de entrevista n.º 1

Rodrigo Miguel Rosa Rodrigues

De: ISCPSI - Direcção Ensino
Enviado: 16 de janeiro de 2026 11:42
Para: Rodrigo Miguel Rosa Rodrigues
Cc: Artur Miguel Soares Pestana
Assunto: FW: Solicitação de colaboração: Dissertação de mestrado em Segurança Pública / AOP Rodrigo Rodrigues
Anexos: Of. AOP Rodrigo Rodrigues.pdf; Solicitação de colaboração - 159150.pdf

Sinal. de seguimento: Flag for follow up
Estado do sinalizador: Sinalizado

Exmo. Sr. Aspirante Rodrigo Rodrigues,
Bom dia,

Encarrega-me o Exmo. Sr. Subintendente Artur Pestana, de dar conhecimento do Despacho de Sua Excelência o Diretor Nacional Adjunto (UORH), para a realização das diligências tidas por convenientes.

Com os melhores cumprimentos,
"Presente pela Proximidade, Próxima na Segurança!" – Estratégia PSP 2025-2027
Direção de Ensino

Instituto Superior de Ciências Policiais e Segurança Interna

www.psp.pt | www.iscpsi.pt

PT

Herminia, Chefe

De: DN DF - Núcleo de Cooperação e Assessoria Técnica <ncat.df@psp.pt>
Enviada: 16 de janeiro de 2026 11:36
Para: ISCPSI - Direcção Ensino <de.iscpsi@psp.pt>
Cc: Rodrigo Miguel Rosa Rodrigues <rmirodrigues@psp.pt>
Assunto: FW: Solicitação de colaboração: Dissertação de mestrado em Segurança Pública / AOP Rodrigo Rodrigues

Exmo. Senhor
Diretor do ISCPSI

Relativamente ao assunto em epígrafe encarrega-me o Exmo. Senhor Diretor do Departamento de Formação, Superintendente Nuno Poiares, de remeter a V. Ex.ª o despacho de Sua Excelência o Diretor Nacional Adjunto (UORH), i.e.:

""Autorizado, mediante a disponibilidade dos oficiais identificados.
Antes da devolução ao ISCPSI, deve previamente ser consultado o GDN."

1

A.3. Ofício com pedido de autorização de realização de entrevista n.º 2

MINISTÉRIO DA ADMINISTRAÇÃO INTERNA
POLÍCIA DE SEGURANÇA PÚBLICA
INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS
E SEGURANÇA INTERNA

Exmo. Sr. Diretor Nacional Adjunto, para a UORH,
MI Superintendente-Chefe Ismael Pereira Gaspar Jorge

Assunto: Solicitação de realização de entrevistas no âmbito da dissertação de mestrado

Eu, Rodrigo Miguel Rosa Rodrigues, Aspirante a Oficial de Polícia finalista do Curso de Mestrado em Segurança Pública, no âmbito da realização da dissertação de mestrado intitulada "Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal", sob orientação do(a) Superintendente-Chefe (Doutor) Luís Manuel Elias e coorientação do Superintendente-Chefe José Emanuel de Matos Torres e Intendente Tito Eurico Faria Fernandes, venho mui respeitosamente solicitar a V.ª Ex.ª autorização:

Para a realização das seguintes entrevistas:

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

A realização destas entrevistas tem como intuito enriquecer a investigação com contributos críticos e fundamentados com base no conhecimento especializado e experiência operacional dos entrevistados. Deste modo, poderá atingir-se uma base mais sólida de análise sobre a pertinência de criação e operacionalização de uma componente de inteligência policial integrada no Corpo de Segurança Pessoal.

Comprometo-me a manter a confidencialidade dos dados recolhidos, fora do âmbito da elaboração e discussão da dissertação, bem como a cumprir as demais regras éticas relativas à realização de investigação científica.

A.4. Despacho de autorização para realização de entrevista n.º 2

Rodrigo Miguel Rosa Rodrigues

De: ISCPSI - Direcção Ensino
Enviado: 3 de fevereiro de 2026 14:50
Para: Rodrigo Miguel Rosa Rodrigues
Cc: Artur Miguel Soares Pestana
Assunto: FW: Solicitação de colaboração: Dissertação de mestrado em Segurança Pública / AOP Rodrigo Rodrigues
Anexos: 2. Of. AOP Rodrigo Rodrigues.pdf; 2. Solicitação_de_colaboração_159150.pdf

Exmo. Sr. Aspirante Rodrigo Rodrigues,

Boa tarde,

Encarrega-me o Exmo. Sr. Subintendente Artur Pestana, de dar conhecimento do Despacho de Sua Excelência o Diretor Nacional Adjunto (UORH), para a realização das diligências tidas por convenientes.

Com os melhores cumprimentos,

"Presente pela Proximidade, Próxima na Segurança!" – Estratégia PSP 2025-2027

Direção de Ensino

POLÍCIA SEGURANÇA PÚBLICA

Instituto Superior de Ciências Policiais e Segurança Interna

www.psp.pt | www.iscpsi.pt

PT

Hermínia, Chefe

De: DN DF - Núcleo de Cooperação e Assessoria Técnica <ncat.df@psp.pt>
Enviada: 3 de fevereiro de 2026 14:32
Para: ISCPSI - Direcção Ensino <de.iscpsi@psp.pt>
Cc: DN DIP <dip@psp.pt>; UEP - Núcleo Doutrina Formação Conjunta <uep.ndfc@psp.pt>; Rodrigo Miguel Rosa Rodrigues <rmirodrigues@psp.pt>
Assunto: FW: Solicitação de colaboração: Dissertação de mestrado em Segurança Pública / AOP Rodrigo Rodrigues

Exmo. Senhor
Diretor do ISCPSI

Exmo. Senhor
Diretor do DIP

Exmo. Senhor
Comandante da UEP

Relativamente ao assunto em epígrafe encarrega-me o Exmo. Senhor Diretor do Departamento de Formação, Superintendente Nuno Poiares, de remeter a V. Ex.ª o despacho de Sua Excelência o Diretor Nacional Adjunto (UORH), i.e.:

"Autorizado, nos termos propostos."

1

Apêndice B – Termo de Consentimento Informado

Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal

Instituto Superior de Ciências Policiais e Segurança Interna

Termo de Consentimento Informado

Tomei conhecimento de que o **Aspirante a Oficial de Polícia Rodrigo Miguel Rosa Rodrigues**, no âmbito da conclusão do Mestrado em Segurança Pública do Instituto Superior de Ciências Policiais e Segurança Interna, se encontra a desenvolver um estudo com o tema **"Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal"**, sob a orientação do Superintendente-Chefe (Doutor) Luís Manuel Elias e a coorientação do Superintendente-Chefe José Emanuel Matos Torres e Intendente Tito Eurico Miranda Fernandes. Fui informado(a) de que a minha colaboração é solicitada através da prestação de declarações em entrevista por escrito, via presencial ou por videoconferência.

Fui informado de que a entrevista será gravada para facilitar a posterior análise, sendo as minhas declarações transcritas de forma integral para a presente dissertação de mestrado. A minha participação terá carácter voluntário, podendo eu, em qualquer momento, recusar responder a determinadas questões ou desistir da entrevista, sem qualquer consequência. Fui ainda informado que não irá existir qualquer tipo de remuneração ou custo associado à participação neste estudo. Fui elucidado sobre todos os aspetos associados à minha participação e tive resposta a todas as questões por mim colocadas.

Desta forma, aceito participar nesta investigação e assino o presente documento como forma de o comprovar.

O Investigador

Assinado por: **Rodrigo Miguel Rosa Rodrigues**
Num. de Identificação: 14619109
Data: 2026.02.17 23:03:59+00'00'

Aspirante a Oficial de Polícia M/159150

O Entrevistado

Lisboa, ____ de _____ de 2026

Apêndice C – Guião de Entrevistas

Instituto Superior de Ciências Policiais e Segurança Interna

Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal

Agradecimento e Introdução:

Gostaria de agradecer o facto de ter aceitado participar neste estudo. Eu sou o Aspirante a Oficial de Polícia Rodrigo Rodrigues e esta entrevista enquadra-se na investigação científica intitulada "Inteligência Policial no Apoio à Atividade Operacional da Segurança Pessoal".

Realizada no âmbito do 38.º Curso de Formação de Oficiais de Polícia, do Mestrado em Segurança Pública do Instituto Superior de Ciências Policiais e Segurança Interna, sob a orientação do Superintendente-Chefe (Doutor) Luis Manuel Elias e a coorientação do Superintendente-Chefe José Emanuel Matos Torres e Intendente Tito Eurico Miranda Fernandes.

Enquadramento e Objetivos:

Com a presente entrevista pretende-se obter contributos que permitam caraterizar o modo como a inteligência policial apoia (ou pode apoiar) a atividade operacional do Corpo de Segurança Pessoal.

Os resultados desta entrevista serão utilizados para responder aos objetivos específicos do estudo, designadamente:

- Analisar a forma como a informação é atualmente recolhida, tratada e partilhada para apoio à atividade operacional da Segurança Pessoal;
- Identificar eventuais lacunas de articulação interinstitucional que condicionem a eficácia do CSP;
- Compreender em que medida existem práticas estruturadas de contrainformação e desinformação no âmbito do sistema de informações do CSP;
- Perspetivar prioridades e implicações da criação de uma componente de inteligência policial especificamente dedicada a apoiar a atividade operacional de Segurança Pessoal.

Guião de Entrevista:

Nome: Clique ou toque aqui para introduzir texto.

Idade: Clique ou toque aqui para introduzir texto.

Categoria Profissional: Clique ou toque aqui para introduzir texto.

Função que desempenha: Clique ou toque aqui para introduzir texto.

Tempo de experiência numa função ligada ao CSP ou às Informações na PSP: Clique ou toque aqui para introduzir texto.

Tempo de serviço na PSP: Clique ou toque aqui para introduzir texto.

A entrevista é composta pelas seguintes questões:

Questões sobre realidade atual:

1. Quando assumem uma missão operacional, os polícias do CSP recebem briefings e/ou elementos escritos ou verbais na área da Inteligência Policial sobre o contexto operacional (perfil do protegido, ambiente, ameaças, vulnerabilidades)? Se sim, de que fonte e de que forma?

Clique ou toque aqui para introduzir texto.

2. No âmbito da formação inicial ou contínua e no exercício diário das funções, os polícias do CSP no terreno são orientados para a recolha de informação de diferentes fontes (segurança de área, população, fontes abertas, redes sociais, etc.) para apoiar a produção de informações relevantes para a atividade operacional da PSP?

Clique ou toque aqui para introduzir texto.

3. Na sua experiência profissional, em operações que implicam o empenhamento do CSP, sente que existem lacunas na partilha de informação entre o CSP e outras subunidades e entidades? Em caso afirmativo, pode descrever situações concretas em que essas lacunas tenham condicionado a eficácia da proteção?

Clique ou toque aqui para introduzir texto.

4. Do ponto de vista da proteção de altas entidades, em que medida considera que atualmente existem (ou não) práticas estruturadas de contrainformação e desinformação integradas no sistema de informações do CSP?

Clique ou toque aqui para introduzir texto.

Questões sobre soluções:

5. Se existisse uma componente de Inteligência Policial especificamente dedicada a apoiar o CSP, que prioridades operacionais e táticas deveria ter?

Clique ou toque aqui para introduzir texto.

6. Que alterações organizacionais, procedimentais ou tecnológicas considera essenciais para que as informações relevantes circulem de forma mais fluida e útil entre quem produz Inteligência Policial e quem comanda ou executa operações de Segurança Pessoal, bem como entre estes e as unidades policiais territorialmente competentes?

Clique ou toque aqui para introduzir texto.

7. Na sua opinião, que tipo de atividades específicas de contrainformação e desinformação deveriam ser desenvolvidas ou reforçadas no âmbito do sistema de informações do CSP, e de que forma essas atividades poderiam contribuir para potenciar a eficácia da proteção de altas entidades e de outras pessoas que beneficiam de segurança pessoal?

Clique ou toque aqui para introduzir texto.

Apêndice D – Entrevista E1

Codificação do Entrevistado: E1

Função: Oficial Superior com experiência na Direção Nacional, Segurança Pessoal e Informações da PSP

Entrevistador: Rodrigo Miguel Rosa Rodrigues

Ano: 2026

1. Os polícias do CSP recebem briefings e/ou elementos escritos ou verbais na área da inteligência policial sobre o contexto operacional? Se sim, de que fonte e de que forma?

Aquilo que era a prática normal relativamente à atuação do CSP, no que tem a ver com a inteligência policial, e falo do tempo em que fui comandante do CSP, era o seguinte: Não há missão nenhuma que não tenha um briefing de situação. Esse briefing tem que incluir a situação do protegido, as vulnerabilidades que possam existir, ou que não existiam ontem e existem hoje, por exemplo, porque surgiu uma ameaça, o ambiente em que se vai operar e as vicissitudes desse ambiente, seja no estrangeiro ou em território nacional. Inclui também aquilo que são as ameaças conhecidas diretamente em relação ao protegido, quer sejam de conhecimento próprio, quer sejam resultantes de informação de *intelligence* produzida pelos serviços de informações e que nos é transmitida. Depois, toda a análise que é feita do ambiente das deslocações, das vulnerabilidades, do histórico que existe relativamente ao local, à entidade, à tipologia de ameaças e às situações inopinadas que podem acontecer, porque isso também pode constituir uma ameaça. Tudo isto tem que ser sempre tido em consideração em qualquer missão operacional.

Estas missões têm que ter planos de execução: um plano principal e planos alternativos. Isto aplica-se aos alojamentos, aos itinerários, às viaturas, aos locais das deslocações, tudo tem que estar pensado. Tem que se pensar nas questões de segurança sanitária, nas evacuações, na possibilidade de um ataque, onde está o backup, o que pode acontecer. Tudo isto tem que ser equacionado.

Do ponto de vista da *intelligence*, o essencial é a capacidade de antecipar. E isso faz-se através de uma recolha permanente de informações, da análise contínua do ambiente.

Muitas vezes, quando estamos a nível local, essa informação passa pelo contacto com entidades locais e pelas equipas avançadas, que têm uma perceção real do terreno.

E muitas vezes essas equipas não podem ir apenas uma hora antes, têm que ir no dia anterior, estar no terreno, fazer essa análise, perceber o ambiente que vão encontrar, estabelecer contactos com a polícia local, com a GNR, com quem for necessário, e articular a operação.

Existia um núcleo de informações que fazia esse processamento e, quando surgiam dados novos ou relevantes, essa informação era comunicada às equipas, mesmo que já estivessem em missão. Esse núcleo de informações estava inserido na UEP inserido no CSP. Era esse o modelo. Este modelo, de recolha permanente de informação e processamento contínuo, é o mínimo que deve existir.

Tem que haver sempre um mecanismo permanente de recolha e tratamento de informação que permita antecipar cenários, seja o 10 de Junho, seja uma visita, seja qualquer evento. Todos os cenários têm que ser antecipados.

2. No âmbito da formação e exercício das funções, os polícias do CSP no terreno são orientados para a recolha de informação como forma de apoio à produção de informações relevantes para a atividade operacional da PSP?

O que acontece com as equipas, ou com os elementos é o seguinte: Os elementos que trabalhavam isolados respondiam perante o chefe de núcleo, seja de entidades nacionais, entidades estrangeiras ou proteção de testemunhas. E, necessariamente, esses núcleos tinham que ter a capacidade de processamento da informação e de comunicação daquilo que chegava e que era relevante para aquele elemento ou para aquela equipa.

Com trabalho em equipa, torna-se mais fácil a perceção do ambiente, porque há mais gente a observar, a interpretar, há uma maior capacidade de leitura do contexto.

Quem está isolado também tem essa responsabilidade. Vai-se apercebendo do que é normal e do que não é normal, daquilo que constitui padrão e daquilo que representa uma alteração de padrão. E a indicação é clara: sempre que há alteração de padrões, e essa alteração pode representar uma ameaça, seja ela imediata ou próxima, deve haver uma comunicação imediata, para que possam ser adotadas as medidas de segurança necessárias. Isto implica uma responsabilidade dupla: por um lado, de quem tutela aquela equipa, relativamente à informação que deve ser tratada e reportada com interesse; por outro lado, dos próprios elementos que estão no terreno, na perceção do ambiente em que operam.

Se houver alterações à normalidade, novos padrões, novos vetores de ameaça, isso tem que ser identificado. Por exemplo, numa deslocação habitual, se algo se altera, já não posso fazer o itinerário normal. Tenho que alterar o percurso e esse novo itinerário tem que ser

avaliado. E o elemento no terreno tem que ter iniciativa para pedir isso, nem que seja no momento. Hoje em dia isso é mais fácil, com ferramentas como o "Google Maps", mas isso não resolve tudo. Portanto, este contacto tem que existir sempre. E há uma responsabilidade que é de ambos: do serviço, mas também das equipas e dos elementos que estão no terreno.

3. Na sua experiência, em operações de segurança pessoal, sente que existem lacunas na partilha de informação entre as subunidades e o CSP e entidades?

Há sempre, ou há uma tendência natural, para poder haver falhas na transmissão de informação, ou transmissão incompleta de informação. Porquê? Porque toda a gente tem muita tendência para entrar na lógica da reserva da informação, no princípio da "necessidade de conhecer", etc.

Mas depois há outra dimensão, que é a falta de perceção de que determinados dados são relevantes para outros. Ou seja, o SIS comunica efetivamente os graus de ameaça relativamente às entidades, às pessoas, isso é feito. Mas essa comunicação é feita num determinado contexto, que é o contexto da análise que o serviço faz. São identificadas ameaças conhecidas — podem ser estas, aquelas —, são analisados eventos, contextos de contestação à postura da entidade, possíveis manifestações, entre outros fatores. Isso faz parte da análise. Mas depois podem existir outras situações que derivam, por exemplo, da vida pessoal, familiar ou social das entidades, que podem não ser imediatamente percetíveis. Muitas vezes, essas situações só são identificadas no terreno.

E depois há situações em que entram várias unidades na operação. Sabe-se que há uma deslocação de uma entidade, que houve reconhecimentos, ações preparatórias, alterações ao planeamento, mas nem sempre existe, por parte de quem está no terreno em relação ao CSP, a perceção de que essas alterações são significativas para a operação de segurança pessoal.

Por exemplo, pode ser relevante garantir que uma determinada área está esterilizada a uma certa hora e que se mantém assim até à chegada da entidade. Tem que ser feito antes, no momento definido, para garantir que a área está efetivamente segura e que não existem no seu interior potenciais ameaças.

Portanto, muitas vezes diria que há transmissão de informação, mas pode ser incompleta. E, por vezes, há também uma perceção insuficiente sobre o que é efetivamente relevante para o CSP, para que a missão possa ser executada com plenitude ou, pelo menos, reduzindo e mitigando os fatores de risco.

4. Do ponto de vista da proteção de altas entidades, considera que atualmente existem (ou não) práticas estruturadas de contrainteligência e/ou contrainformação no CSP?

Podem existir situações em que, para garantir maior segurança nas deslocações ou reduzir vulnerabilidades, se transmite informação incompleta. Por exemplo, pode anunciar-se um determinado itinerário e depois utilizar-se outro. Pode indicar-se uma hora de chegada a um local e depois essa hora ou local serem diferentes na prática. Essas são práticas que visam reduzir vulnerabilidades, antecipar situações menos positivas ou potencialmente prejudiciais. Portanto, isso pode acontecer. É equivalente, por exemplo, à utilização de várias viaturas semelhantes numa coluna, em que não se sabe exatamente em qual delas segue a entidade.

Nesse sentido, sim, são práticas utilizadas. Não têm nada de extraordinário nem de ilegítimo, têm um objetivo operacional claro. Não se trata de "enganar" por si só, mas sim de proteger a operação.

5. Se existisse uma componente de inteligência policial especificamente dedicada a apoiar o CSP, que prioridades operacionais e táticas deveria ter?

Tem que existir, dentro do CSP, uma unidade ou uma capacidade de produção de *intelligence* que consiga, desde logo, recolher informação, ou, pelo menos, receber informação das várias fontes. Isso inclui os relatórios dos serviços de informações, aquilo que sejam ameaças criminais identificadas pelo DIP ou pela Investigação Criminal. Depois, tem que haver a capacidade de processar toda essa informação e de a difundir internamente, de forma adequada, pelas equipas. Mas, além disso, tem que existir capacidade tecnológica que permita detetar ameaças ou, pelo menos, identificá-las com antecedência suficiente para as neutralizar. Tudo isto permite garantir segurança sem depender exclusivamente de recursos humanos, complementando-os com tecnologia.

Hoje, com as tecnologias disponíveis, qualquer deslocação pode ser georreferenciada. É possível identificar previamente circuitos alternativos, locais de recolha, rotas de fuga e alternativas em caso de necessidade, incluindo soluções de alojamento. Tudo isso faz parte da *intelligence*.

A capacidade de processamento da *intelligence* é indissociável da atividade operacional, têm que funcionar em paralelo. O planeamento de uma missão tem que ser completo: não é apenas a componente operacional da deslocação, mas também todo o enquadramento informacional.

Tem que haver também a capacidade de projetar elementos no terreno que se integrem no ambiente, muito antes da chegada da entidade, recolhendo informação. Para além das equipas avançadas que fazem o trabalho imediato, é necessário ter capacidade de adaptação em função da informação recolhida

Os cenários têm que ser sempre planeados. Há um programa definido, mas para cada etapa tem que se equacionar: "o que pode acontecer aqui?" e, se acontecer, "o que fazemos a seguir?"

Mas há ainda um aspeto fundamental: o chefe de equipa, ou quem está no terreno, tem que ter poder de decisão sobre um conjunto de situações. E isso nem sempre acontece. Esse responsável tem que poder alterar um itinerário, mudar uma entrada, ou até influenciar alterações ao programa por razões de segurança. Isso é determinante.

Não pode estar dependente de pedir autorização à central ou ao comando para tudo. A decisão pode ser comunicada e validada posteriormente, mas há situações em que tem que ser tomada no momento.

6. Que alterações considera essenciais para que as informações circulem de forma mais eficaz entre quem produz inteligência policial e quem comanda ou executa operações de segurança pessoal e entre estes e as Unidades Policiais territorialmente competentes?

Eu acho que aquilo que tem que existir é um fluxo de informação contínuo, ou seja, tem que haver uma circulação de informação eficaz. E isso implica que exista uma perceção real do que podem ser vetores de ameaça. Isto não se refere tanto ao SIS, porque esses têm isso bem definido. O problema está muitas vezes na forma como esses vetores de ameaça se manifestam, que nem sempre é facilmente compreendida por todos. E, não havendo essa perceção, não há comunicação, não há fluxo. Muitas vezes é isso que acaba por bloquear a circulação da informação.

Outras vezes, a questão é o tempo de processamento. A informação pode chegar, mas não há tempo para a ler ou analisar e, portanto, não é transmitida. E, quando é transmitida, já tem pouca ou nenhuma utilidade. Isto tem muito a ver com a gestão do tempo e com a oportunidade da comunicação. Isto leva a que, numa deslocação ou num programa, a própria estrutura que acompanha tenha que ter capacidade de projeção para antecipar alterações que não tenham sido comunicadas. Daí a existência de equipas avançadas. Mas deve existir sempre a possibilidade de projeção de uma equipa de *intelligence*, que possa atuar no terreno, utilizar meios tecnológicos, como câmaras instaladas, e avaliar previamente determinados locais. Isso

reforça as inspeções desenvolvidas, por exemplo, pelo CIEX, que assegura a verificação e estabilização dos locais.

Tendo em conta o princípio da especialização, e sendo esta uma área muito específica, essa equipa deveria estar ligada ao CSP. Ainda que possa estar integrada numa estrutura de *intelligence* mais alargada, pela especificidade da função e da informação, deveria estar diretamente associada ao CSP.

7. Na sua opinião, que tipo de atividades específicas de contrainteligência e contrainformação poderiam ser desenvolvidas ou reforçadas no âmbito do sistema de informações do CSP para potenciar a eficácia da proteção de altas entidades e de outras pessoas que beneficiam de segurança pessoal?

Há um conjunto de medidas preventivas que devem ser adotadas. Por exemplo, a agenda não é divulgada com uma semana de antecedência. Os itinerários não são divulgados. Os veículos das entidades, por exemplo, são guardados em garagens, em locais seguros. Portanto, há um conjunto de medidas preventivas que devem ser adotadas nesse âmbito.

E muitas dessas medidas acabam por inibir a necessidade de recorrer a ações de desinformação ou a medidas alternativas. Porquê? Porque, se já se acautelou previamente o risco, reduz-se a necessidade de recorrer a esse tipo de soluções.

Apêndice E – Entrevista E2

Codificação entrevista: E2

Função: Oficial com função de comando no CSP

Tempo de experiência numa função ligada ao CSP ou às Informações na PSP: 11 anos

Tempo de serviço na PSP: 36 anos

Entrevistador: Rodrigo Miguel Rosa Rodrigues

Ano: 2026

1. Os polícias do CSP recebem briefings e/ou elementos escritos ou verbais na área da inteligência policial sobre o contexto operacional? Se sim, de que fonte e de que forma?

Sim. Embora a minha prioridade seja sempre a salvaguarda da integridade da segurança operacional e a proteção de informações sensíveis e dos Protegidos, posso informar que o CSP utiliza uma ampla variedade de fontes seguras e confiáveis, em conformidade com os protocolos normativos e operacionais estabelecidos na PSP, de modo a garantir a eficácia das nossas missões. Detalhes específicos sobre essas fontes ou métodos não podem ser divulgados por razões de segurança e proteção de procedimentos operacionais mas, em regra, resultam de produção informacional própria/interna e/ou tramitam pelo SINTEL/PSP e/ou pela Plataforma Partilhada de Operações de Segurança do SSI (PPOS).

2. No âmbito da formação e exercício das funções, os polícias do CSP no terreno são orientados para a recolha de informação como forma de apoio à produção de informações relevantes para a atividade operacional da PSP?

Sim, é um procedimento sistemático e permanente.

3. Na sua experiência, em operações de segurança pessoal, sente que existem lacunas na partilha de informação entre as subunidades e o CSP e entidades?

No início de cada serviço de segurança pessoal e/ou de Proteção Policial, o CSP já se encontra guarnecido de todos os elementos de informação necessários ao desenvolvimento da sua atividade operacional, seja através de produção própria e/ou sob apoio do SINTEL/PSP e/ou da PPOS, incluindo a implementação das medidas de segurança adicionais por parte do dispositivo securitário nacional que o CSP considere necessárias (envolvendo sempre a prévia designação de Pontos Operacionais de Contacto - POCs), não havendo margem para lacunas

que condicionem a eficácia da ação do CSP. Genericamente, o mesmo se aplica à produção de avaliações de risco dinâmicas e aos ajustes operacionais que, entretanto, se impuserem.

4. Do ponto de vista da proteção de altas entidades, considera que atualmente existem (ou não) práticas estruturadas de contrainteligência e/ou contrainformação no CSP?

Embora importe garantir a integridade da segurança operacional, admito que existem práticas estruturadas incluídas nos pacotes de planeamento operacional do CSP e, tendo em consideração o dinamismo da evolução das ameaças (ex: tipos e formas), são de igual forma desencadeadas ações híbridas e ciber.

5. Se existisse uma componente de inteligência policial especificamente dedicada a apoiar o CSP, que prioridades operacionais e táticas deveria ter?

Não confirmando ou infirmando a existência dessa capacidade, a sustentação de contramedidas, operacionais e/ou de (contra)inteligência policial, em especial o desenvolvimento de ações de contravigilância e a monitorização de ciber e tecnoameaças, são essenciais/prioritárias para o CSP.

6. Que alterações considera essenciais para que as informações circulem de forma mais eficaz entre quem produz inteligência policial e quem comanda ou executa operações de segurança pessoal e entre estes e as Unidades Policiais territorialmente competentes?

Nada especialmente critico. Sobretudo, existe uma especial carência ao nível do investimento/desenvolvimento tecnológico.

7. Na sua opinião, que tipo de atividades específicas de contrainteligência e contrainformação poderiam ser desenvolvidas ou reforçadas no âmbito do sistema de informações do CSP para potenciar a eficácia da proteção de altas entidades e de outras pessoas que beneficiam de segurança pessoal?

O desenvolvimento e aprimoramento de ações de contravigilância e de contramedidas face a ciberameaças e tecnológicas carecem de constante reforço, designadamente por mitigarem vulnerabilidades resultantes de indesejadas rotinas e pela exposição digital/tecnológica natural/decorrente dos tempos modernos.

Apêndice F – Entrevista E3

Codificação do Entrevistado: E3

Função: Oficial com funções no Departamento de Informações Policiais

Tempo de experiência numa função ligada ao CSP ou às Informações na PSP: 2 anos

Tempo de serviço na PSP: 8 anos

Entrevistador: Rodrigo Miguel Rosa Rodrigues

Ano: 2026

1. Os polícias do CSP recebem briefings e/ou elementos escritos ou verbais na área da inteligência policial sobre o contexto operacional? Se sim, de que fonte e de que forma?

Há vários caminhos. E, portanto, falando por exemplo de altas entidades, o processo dá início com um pedido ao SSI para se corresponder com o SIS para efeitos de avaliação da ameaça. São eles que, do ponto de vista legal, tem essa competência e utilizam a uma as ferramentas que têm fazerem a avaliação do grau de ameaça que está implícita sobre aquela pessoa. E consoante o grau de ameaça que está de acordo também com o plano coordenador dos Serviços das Forças de Segurança, há um conjunto de medidas de segurança obrigatórias e facultativas.

Complementarmente a isso, falamos também de informações classificadas. Portanto, há um canal de transmissão e essa informação é-nos devolvida com a avaliação da ameaça por parte do tal serviço que está autorizado e com competência para fazer do ponto de vista legal em território nacional e nós complementamos com uma avaliação do risco. Não é a mesma coisa, é complementar, e é isso que depois deve servir de base para tentar torná-lo mais operacional naquilo que é a colheita da informação e depois se tenta transmitir ao CSP. Faz-se o relatório, mais uma vez, a informação classificada vai pelos canais que estão definidos como tal, e chega à UEP.

Portanto, isto é o que é feito e, nessa avaliação do risco, o objetivo é colecionar, recolher tudo o que tenha acontecido sobre aquela pessoa, o histórico passado, coisas que poderão eventualmente levar-nos a considerar uma avaliação do risco.

Tem que ser mais ou menos assim e, portanto, fazemos uma avaliação *open source* ou não, com todas as ferramentas que temos. É essa a nossa missão nas informações, na inteligência da polícia, onde conseguimos e onde vamos colocar tudo aquilo que encontrámos ao nível dos agentes da ameaça, para tentar, de alguma forma, enquadrar os operacionais.

Isso é importante dizer, aliás, é uma das muitas coisas que às vezes vemos quando existe este tipo de briefing que antecede o início da implementação do serviço de segurança pessoal. A informação é ministrada para eles usarem e tentarem usar em seu benefício próprio. Não é só da entidade, mas deles próprios, porque eles, colateralmente, também podem ser visados pelo agente da ameaça e, obviamente, a segurança da pessoa está inteiramente interdependente da segurança destes profissionais.

Queremos rever muitas coisas, nomeadamente a NEP que regula a forma como a PSP se articula no caso da proteção de testemunhas, porque há situações com enquadramentos jurídicos específicos que obrigam ao envolvimento de autoridades judiciárias e, portanto, a coisa processa-se de forma diferente.

Este serviço de inteligência projeta-se no terreno com o serviço de segurança pessoal. Nós utilizamos o termo Proteção Policial, que é o que também está definido, mas que tem falhas e podemos falar sobre isso, porque é uma das coisas que queremos rever.

Por exemplo, ainda agora tivemos numa situação com carácter de sensibilidade muito maior. Porquê? Porque estava subjacente uma relação de ameaça enorme, sinalizada pelo serviço competente, e nós, na avaliação do risco, também confirmámos que a ameaça ou risco subjacente àquela situação era muito maior.

Havia pessoal do CSP de todas as categorias hierárquicas porque entendemos que temos que ir ao patamar dos chefes de equipa, porque são eles que estão diretamente no terreno. Complementarmente, acrescentámos mais informação, porque o nosso trabalho de inteligência identificou o agente de ameaça, as suas particularidades, as suas formas de ação.

No caso concreto, estávamos a falar de alguém em regime de proteção de testemunhas, que tem enquadramento legal próprio. Tudo o que vai fora daí fica numa zona cinzenta. Pode atribuir-se um efeito analógico àqueles processos, mas depende das pessoas e isso depois condiciona os processos.

Da minha parte, enquanto pessoa com funções de coordenação deste núcleo e o próprio CSP também partilha desta opinião, há um trabalho que é feito no sentido de isto ser para proveito de todos. É um trabalho conjunto. No final é a PSP que está em causa, a reputação da polícia, a segurança das pessoas, a segurança do Estado.

2. No âmbito da formação e exercício das funções, os polícias do CSP no terreno são orientados para a recolha de informação como forma de apoio à produção de informações relevantes para a atividade operacional da PSP?

Do ponto de vista das competências, elas estão institucionalmente. Agora, do ponto de vista das competências que lhes são atribuídas, os polícias do CSP não estão formados, a priori, para isto.

Mas isto não deixa de ser uma ciência. Implica formação, implica conhecimento. Para fazer este trabalho de análise de informações, e nós estamos a fazer esse caminho aqui no Departamento de Informações, é necessário ter muita formação, ter as ferramentas e o conhecimento para o poder fazer.

Portanto, eu não sei se eles têm essa indicação ou não. Duvido que tenham essa capacidade e capacitação. Agora, do ponto de vista da formação, não sei como é que está neste momento. Mas, sem dúvida alguma, que, por exemplo, no caso do CSP, faz todo o sentido que na formação deles, no curso, tenham uma maior componente nesta área, nem que seja para sensibilizar. Porque depois, do outro lado, quem está no terreno é o efetivo.

E às vezes temos que lembrar que há certas regras que estão definidas e têm que ser cumpridas. Por exemplo, eles são obrigados a remeter informações mensalmente. Portanto, são instruídos. Mas é um trabalho que implica formação.

Posso dizer que, no ano passado que o comandante do CSP, fez isso e nós ficámos incluídos, e deduzo que até com algum peso, na formação anual que foi feita no CSP.

É essencial trabalhar na sensibilidade do efetivo para, no local, não desconsiderarem certas coisas ao nível das informações.

Faz sentido, sem dúvida. Aliás, até na perspetiva contrária, na contrainteligência fazia sentido eles também terem algum retorno, algum enquadramento sobre como é que nós trabalhamos, para depois se encontrarem. Porque na contravigilância, por exemplo, isso tem que acontecer, eles têm que perceber o que é que cada um faz, como é que faz, e estar coordenados.

3. Na sua experiência, em operações de Segurança pessoal, sente que existem lacunas na partilha de informação entre as subunidades e o CSP e entidades?

Eu acho que às vezes nos falta, e começando por aí, a coordenação, com base em exemplos práticos de coisas que estão a acontecer ou que já aconteceram, algumas ainda a decorrer.

A coordenação começa logo numa fase inicial. As pessoas e os serviços têm que ter consciência do que é que cada um faz e cada um deve fazer o seu papel. Só isso. Às vezes há atropelos, um já está a assumir uma função que não é a sua, outro já está a assumir outra, ou

estão os dois a assumir a mesma função. Isso, obviamente, traz consequências a nível interno, falhas de informação, desencontros, o que for.

E, naturalmente, também traz consequências para fora, quando nessas situações estão envolvidos outros serviços ou outras entidades. Portanto, claramente que sim.

Dou-te um exemplo no nosso caso, para perceberes. Se na polícia está instituído que tudo o que diga respeito a proteção de testemunhas deve ser comunicado para processamento e coordenação ao serviço de Proteção Policial, onde está incluído o serviço de segurança pessoal, faz sentido que, por exemplo, o Conselho Superior da Magistratura, que é um órgão superior na magistratura e responsável por ter conhecimento de tudo o que possa colocar em risco ou perigo a segurança e a vida dos seus funcionários, principalmente dos juízes, canalize toda a informação sensível para esse serviço.

Qual é o nosso trabalho, e o que temos feito? Reunir com as pessoas e explicar que, na PSP, o caminho é este, o canal é este. É para aqui que enviam, só para aqui. Porque, senão, o que acontece? Enviam uma informação sensível, que contém dados sobre agentes da ameaça, o que fazem, o que não fazem, onde estão, e que pode conter também dados sobre possíveis alvos, que às vezes estão na polícia, outras vezes na própria estrutura, às vezes são altas entidades, com dados pessoais. E essa informação acaba distribuída por toda a gente.

Isso são quebras de segurança enormes. Portanto, é claramente uma questão de coordenação e de organização. Sim, acontece. E acho que o primeiro passo é, de uma vez por todas, sentarem-se, definirem tudo muito bem, terem as coisas estruturadas.

É algo que eventualmente poderás sentir quando fores para a polícia: é uma instituição com muitas valências, mas onde, por vezes, faltam procedimentos claros, faltam manuais, faltam as coisas escritas. Isto não pode depender apenas das pessoas. Tem que haver um modelo definido: é assim que nós trabalhamos, e há uma razão para trabalharmos assim. Uniformizar procedimentos!

4. Do ponto de vista da proteção de altas entidades, considera que atualmente existem (ou não) práticas estruturadas de contrainteligência e/ou contrainformação no CSP?

Eu não sei exatamente como é que eles funcionam, nessa parte não sei. Ou seja, aquilo que é óbvio é que a atividade deles deveria ser enquadrada e trabalhada de forma sigilosa. E isso implica, necessariamente, uma componente de inteligência.

Porque, quando nós falamos deste tipo de pessoas, deste tipo de Estados, deste tipo de associações, estamos a falar de realidades que exigem metodologias e lógicas próprias de trabalho de inteligência. São conceitos e procedimentos que permitem calcular riscos, construir

cenários, perceber exatamente com o que é que estás a lidar e com o que podes contar, para te preparares devidamente para aquele trabalho.

Às vezes, aquilo que temos que fazer, e foi o que aconteceu numa situação que ainda está a decorrer, é reforçar constantemente: atenção às comunicações, atenção à forma como falam entre vocês, ao que dizem e como dizem. Atenção ao que levam convosco quando vão executar o trabalho. Atenção às viaturas que utilizam, às limitações que existem, a determinados pormenores operacionais.

Também compete à contravigilância assumir a sua posição. Não é só dizer que existe, é efetivamente fazer. Se eu digo que faço contravigilância, então tenho que garantir que vocês vão fazer um trabalho de segurança a determinadas pessoas, eu vou fazer um trabalho de segurança a vocês. Vou tentar garantir que não haja ninguém no vosso encalço.

Portanto, a polícia tem que perceber que isto é importante. Tem que perceber que é estratégico. O CSP tem uma missão específica dentro da polícia. E não é só o CSP.

A PSP tem projeção nacional total. E mais, tem que perceber que isto não é matéria com que se brinque. Temos que ter trabalho desenvolvido, planeamento estruturado e as ferramentas necessárias, quer no âmbito da inteligência, quer no terreno, para que o CSP atue como deve ser. E tem que ter recursos neste sentido.

5. Se existisse uma componente de inteligência policial especificamente dedicada a apoiar o CSP, que prioridades operacionais e táticas deveria ter?

Já pensei nisso. Mas também já me disseram, e isto às vezes tem a ver com as pessoas, que quem está num determinado serviço pode achar que o seu caminho e a sua posição deveriam ser outros. Pode querer ser mais independente, estar mais focado naquela área específica. E isto acontece. É a realidade, é a vida institucional.

Por exemplo, o SIS tem projeção nacional. Há países que têm essa forma de organização: um serviço de inteligência a funcionar, que depois tem também uma projeção operacional. E essa projeção operacional, numa lógica de prevenção, poderia ser o CSP, assegurando a segurança pessoal.

Estamos a falar, por exemplo, de proteção de testemunhas no âmbito de processos-crime. Poderíamos ir por aí. Se me perguntasses se isso faria sentido, precisava de estar aqui mais tempo, observar, trabalhar na prática, perceber realmente se isso resultaria ou não. Não é uma proposta simples.

Mas, no modelo atual da PSP, como as coisas estão instituídas, retirar isto, e já nem estou a falar de aplicar noutro lado, não me parece que fosse melhor. Às vezes, o que acontece na polícia é que temos serviços com missões, competências e ferramentas bem definidas, e depois outros departamentos começam a criar algo semelhante, muitas vezes para terem também projeção. E isso, normalmente, tem a ver com a pessoa que lá está. Não é que não possa fazer sentido, mas a questão é que o departamento não trabalha sozinho, nem trabalha para si próprio, trabalha para a instituição.

Na minha ótica, aquilo que existe atualmente na PSP é funcional. Pode não ser perfeito, mas é funcional. Temos capacidades, em algumas áreas mais desenvolvidas, noutras ainda com caminho a fazer, mas estamos a crescer e devemos continuar a melhorar.

Se concordava? Dependeria muito do modelo e da forma como fosse pensado. Mas, no quadro atual, o que existe na PSP faz sentido e é funcional.

6. Que alterações considera essenciais para que as informações circulem de forma mais eficaz entre quem produz inteligência policial e quem comanda ou executa operações de segurança pessoal e entre estes e as Unidades Policiais territorialmente competentes?

Penso mesmo que a solução é de uma vez por todas, firmar-se aquilo que já está escrito sobre isto e ampliar o que está definido.

Há situações que não estão enquadradas no regime de proteção de testemunhas, que é um regime legal próprio, com princípios específicos, aplicável a determinado tipo de pessoas no âmbito de um processo-crime. Nem sempre estamos perante esses casos.

Por isso, deveria centralizar-se isto aqui, a esse nível, de forma clara e definitiva. O CSP, em termos de segurança pessoal, já está centralizado: se fazem segurança pessoal, ninguém faz por eles. Isso está definido.

Tudo o resto, aquilo que na doutrina policial se designa por Proteção Policial, quase como um "chapéu" da segurança pessoal, tudo o que é projeção no terreno, deveria estar igualmente centralizado, incluindo a componente de contravigilância e afins.

Porque a informação tem que ser centralizada. Se tens uns a trabalhar a informação, a recolher e a tratar dados, mas depois tens outros a fazer trabalho operacional sem essa articulação, vais criar dispersão.

O caminho tem sido, cada vez mais, a centralização. O essencial é ter capacidade para fazer isso. E, antes disso, ter capacidade para definir e firmar processos e procedimentos, como é que a coisa deve ser feita, quem faz o quê, por que canal e em que momento.

7. Na sua opinião, que tipo de atividades específicas de contrainteligência e contrainformação poderiam ser desenvolvidas ou reforçadas no âmbito do sistema de informações do CSP para potenciar a eficácia da proteção de altas entidades e de outras pessoas que beneficiam de segurança pessoal?

Nunca me tinham feito essa pergunta, nem tinha pensado nisso.

Eu não sei se eles se deveriam preocupar tanto com isso, ou seja, com a contrainteligência e com a contravigilância. Eu entendo a contravigilância como uma projeção operacional da contrainteligência.

Acho que o mais importante, e foi isso que tentei transmitir, é que a PSP, como um todo, tem estes serviços que trabalham em conjunto, ou que deveriam trabalhar sempre em conjunto, sobretudo nestas situações. Umas são mais sensíveis do que outras, a ameaça pode ser mais latente, o risco mais elevado.

Cabe ao Departamento de Inteligência aprimorar as suas ferramentas, os seus métodos de trabalho e a sua projeção estratégica, mas depois também projetar isso no terreno, através do serviço de contrainteligência e de contravigilância, que funciona como complemento ao serviço de segurança pessoal e ao CSP.

E, obviamente, isto funciona também em sentido inverso. O CSP tem que ter consciência do que é que aqui é feito, como é que é feito, como é que se trabalha, com quem se fala, com quem se coordena. Têm que perceber o que é que nós fazemos e o que é que eles fazem.

Eles devem concentrar-se na segurança pessoal das pessoas que protegem. Pela lógica, e parece-me que faz sentido, aquilo que está "nas costas" deles, do ponto de vista teórico e do que está instituído, deve ser assegurado por nós. É por isso que se chama contrainteligência e contravigilância: aquilo que está por trás, aquilo que não é visível.

Apêndice G – Entrevista E4

Codificação do entrevistado: E4

Função: Oficial com funções de comando operacional num destacamento do CSP

Tempo de experiência numa função ligada ao CSP ou às Informações na PSP: 7 anos

Tempo de serviço na PSP: 13 anos

Entrevistador: Rodrigo Miguel Rosa Rodrigues

Ano: 2026

1. Os polícias do CSP recebem briefings e/ou elementos escritos ou verbais na área da inteligência policial sobre o contexto operacional? Se sim, de que fonte e de que forma?

De uma forma geral, ou seja, não nos focando apenas na minha situação atual, porque neste momento estou a comandar o destacamento de segurança pessoal do Presidente, que acaba por ser uma área diferente, em que trabalhamos apenas com essa entidade, mas olhando para a segurança pessoal no seu todo, tanto no grupo das entidades nacionais como no grupo das entidades estrangeiras, o que normalmente acontece é o seguinte: Não me parece que exista ainda uma relação muito próxima com as informações, ou que nos chegue, de forma sistemática, algum tipo de informação sobre a entidade. Os briefings que acontecem são mais focados na prática operacional, centrados no programa em si, nos itinerários, nos dispositivos que vão ser empenhados na segurança e na eventual coordenação com outras unidades territoriais, designadamente os comandos.

Relativamente à informação sobre a entidade, acho que é algo que tem que partir de nós para conseguirmos obter alguma coisa. Não é algo que, por si só, já venha ou que seja rotina acontecer, nem que a polícia nos apresente de forma estruturada.

2. No âmbito da formação e exercício das funções, os polícias do CSP no terreno são orientados para a recolha de informação como forma de apoio à produção de informações relevantes para a atividade operacional da PSP?

Relativamente à formação do CSP, privilegia-se fortemente a vertente técnica e tática, bem como a forma de colocar essas duas componentes em prática. No que diz respeito à informação, não há uma atenção especial sobre essa matéria.

Acaba por depender muito da iniciativa de cada um fazer essa recolha de informação. Claro que, em termos macro, todos sabemos que, para garantir a qualidade do nosso serviço, temos que fazer essa recolha. No entanto, a forma e o modo como isso deve ser feito ainda

estão um pouco por explorar. Acho que devíamos dar outras bases ao pessoal para realizar essa recolha.

Quando estamos no terreno, há elementos que se focam muito na segurança da área e na caracterização da população — que tipo de população está presente e como é que isso se relaciona com a entidade que vamos proteger. Mas, se calhar, descuramos um pouco a vertente das fontes abertas e das redes sociais. Portanto, não há um caminho uniforme seguido por todos; cada um acaba por fazer aquilo que entende como mais importante. Ou seja, não temos mecanismos padronizados que indiquem como deve ser feita essa preparação, seja numa ação preparatória, seja no próprio dia, momentos antes da chegada da entidade. Não existem orientações claras sobre como estruturar essa recolha de informação.

3. Na sua experiência, em operações de segurança pessoal, sente que existem lacunas na partilha de informação entre as subunidades e o CSP e entidades?

Todos nós conhecemos a orgânica da PSP e sabemos que existe um departamento que se dedica à pesquisa e partilha de informações. No entanto, entre esse departamento e o CSP ainda existe um vazio considerável.

Se calhar, por iniciativa nossa, deveríamos começar a estreitar mais as ligações, neste caso dentro da PSP, entre o DIP e o CSP. Devíamos ser nós a dar os *inputs* sobre aquilo que necessitamos para o nosso serviço, para que o departamento possa, então, orientar a sua pesquisa em função das nossas necessidades.

Digo isto porque, quando há efetivamente necessidade, como aconteceu, por exemplo, na visita do Papa ou na visita do Presidente ucraniano, conseguimos esse apoio. Nesses casos, o departamento consegue fazer a pesquisa de forma direcionada e útil para o nosso serviço.

Por isso, acho que aqui a iniciativa deveria partir da segurança pessoal, procurando junto do DIP, e junto dos restantes serviços, saber o que existe sobre determinada entidade. Se esperarmos que o DIP tome essa iniciativa, pode não acontecer, porque o departamento tem muitos serviços e muitas prioridades. A segurança pessoal acaba por ser apenas um pequeno fator dentro do universo da polícia.

Relativamente ao destacamento de segurança pessoal do Presidente da República, para além do DIP, recorremos também ao SIS, já por várias vezes, em visitas de Estado ou visitas oficiais de Sua Excelência o Presidente da República. Procuramos perceber como está o país de destino, que notícias existem, que informações nos podem ser transmitidas para que possamos adaptar o nosso dispositivo e a nossa forma de atuar nesse contexto.

Isso é uma ajuda bastante relevante, e temos recorrido a esse apoio do SIS tal como do DIP com mais frequência ultimamente. Mas, mais uma vez, tem que partir de nós para que aconteça. Nós pedimos audiências, solicitamos relatórios, e essa informação acaba por ajudar muito o nosso serviço.

4. Do ponto de vista da proteção de altas entidades, considera que atualmente existem (ou não) práticas estruturadas de contrainteligência e/ou contrainformação no CSP?

Não estão identificadas, atualmente nenhumas práticas no âmbito da contrainformação ou desinformação. Na nossa área, na segurança pessoal, sobretudo quando trabalhamos com entidades nacionais e estrangeiras, poderia ser vantajoso existir algo nesse sentido.

No entanto, no caso das entidades nacionais, é um tema difícil de operacionalizar. Podemos facilmente cair no ridículo de tentar aplicar práticas de contrainformação ou desinformação quando a agenda é pública e toda a gente sabe como é que as coisas vão decorrer. Estar a criar contrainformação num contexto em que os dados essenciais já são do domínio público pode tornar-se contraproducente.

Aquilo que efetivamente existe é uma proteção da informação sensível que depende de nós. Por exemplo, os itinerários concretos, os horários podem ser públicos, mas os locais de embarque e desembarque ou determinadas opções operacionais são informação que depende de nós e que procuramos proteger. Essa informação é partilhada apenas internamente, entre quem precisa de a conhecer, tentando sempre que o número de pessoas com acesso seja o mais reduzido possível.

O problema é que trabalhamos com agendas que, umas vezes, são públicas e, outras vezes, privadas, mas pertencem às entidades que protegemos. Apesar da nossa sensibilização para a necessidade de reserva, acabam por partilhar a informação conforme entendem, consoante queiram ou não que determinado evento seja público. E nós ficamos, de certa forma, condicionados por essa vontade.

Temos, por isso, que nos adaptar ao que é decidido pelas próprias entidades e trabalhar em função desse enquadramento.

5. Se existisse uma componente de inteligência policial especificamente dedicada a apoiar o CSP, que prioridades operacionais e táticas deveria ter?

Ora bem, a existir essa componente, acho que deveria, fundamentalmente, produzir avaliações de risco dinâmicas, por evento e por deslocação. Ou seja, não termos algo muito macro e geral, mas algo mais pormenorizado e ajustado a cada serviço.

Depois, teria que se definir onde é que essa componente ficaria integrada, se pertenceria ao DN, se estaria diretamente na estrutura da segurança pessoal, o que até poderia fazer mais sentido, por haver maior sensibilidade para a realidade operacional. Mas, independentemente da tutela, deveria ser uma estrutura dedicada à produção de avaliações de risco, e que essas avaliações teriam que ser dinâmicas. Num só dia podes ter vários eventos e várias deslocações, e todas as avaliações serão diferentes.

Para além disso, deveria haver elaboração de perfis de ameaça individualizados, ponderando sempre o comportamento da entidade protegida e o comportamento da população com quem essa entidade vai interagir.

Outro ponto essencial seria a monitorização contínua de fontes abertas e redes sociais. Hoje em dia, toda a gente partilha tudo, estados de espírito, opiniões, notícias, até desinformação. Ter alguém dedicado a pesquisar nessas fontes, a perceber se existe algum movimento, ainda que pequeno, contra os ideais ou contra a figura da pessoa que estás a proteger, seria extremamente útil.

Também considero importante a identificação prévia de vulnerabilidades estruturais nos locais a visitar. Isso já é feito, mas seria relevante concentrar essa informação numa estrutura ou numa pessoa específica, criando um histórico das localidades. Ainda que as avaliações tenham que ser dinâmicas, é fundamental manter memória institucional sobre os locais. Porque não é igual deslocares-te com o Presidente da República ou com o Primeiro-Ministro ao mesmo local. As avaliações têm que ser diferentes. O perfil da entidade conta muito. O Primeiro-Ministro, por exercer funções executivas, tende a gerar mais controvérsia e polarização do que o Presidente da República.

Todos estes elementos devem servir de apoio à decisão do comandante da missão e devem ser sintetizados em briefing antes do início do serviço.

O ponto essencial é este: é a produção de avaliações de risco e que sejam dinâmicas, porque avaliações de risco existem sempre, não se faz nada sem avaliação. Mas, muitas vezes, não se incorpora devidamente o fator "entidade", que tipo de notícias têm saído sobre ela, que reações pode suscitar, qual é o contexto político ou social do local. Por exemplo, deslocar-se a um concelho com determinado perfil político pode influenciar o ambiente à chegada da entidade. Tudo isso deve ser ponderado. O fundamental é conjugar o perfil da entidade com o

evento específico. Pode ser o mesmo evento, mas gerar situações completamente distintas consoante a entidade presente.

Quando falamos de entidades estrangeiras, o estudo tem que começar ainda mais cedo. A partir do momento em que é comunicada a visita ao nosso país, deve iniciar-se a recolha e preparação da informação, tentando obter o programa o mais antecipadamente possível. A produção de avaliações de risco deve ser ajustada à pessoa que vem e ao contexto que a envolve.

Já tivemos situações que correram bem graças à capacidade de adaptação do pessoal da segurança pessoal, mas, com uma estrutura mais preparada nesta vertente, poderíamos evitar determinadas situações.

6. Que alterações considera essenciais para que as informações circulem de forma mais eficaz entre quem produz inteligência policial e quem comanda ou executa operações de segurança pessoal e entre estes e as Unidades Policiais territorialmente competentes?

A minha sugestão seria, desde logo, a criação de um canal formal e obrigatório de partilha prévia de informação entre as unidades territoriais dos comandos e o CSP, relativamente aos eventos que constam do programa e que dizem respeito às entidades que estamos a proteger.

Depois, a implementação de um modelo normalizado de briefing escrito, com secções obrigatórias. Ou seja, quando é feito um briefing, este não deveria depender apenas de quem o elabora ou do comandante que está à frente do policiamento ou da segurança da entidade. Deveria existir um padrão definido, com tópicos obrigatórios a apresentar. Isto porque, as equipas num dia estão com determinado comandante, noutro dia com outro, mas deveriam saber sempre que secções vão ser abordadas em todos os eventos e serviços em que são empenhadas. Por exemplo, uma secção dedicada a ameaças, outra a vulnerabilidades, contexto social, antecedentes. Esses seriam temas-base. Assim, o serviço estaria sempre estruturado de forma semelhante, o que facilita a assimilação por parte das equipas e garante maior consistência. É mais eficaz trabalhar sempre com o mesmo padrão do que, num dia, o briefing se focar apenas nas ameaças e, noutro, ignorar determinados aspetos relevantes.

Outra medida importante seria a criação de uma plataforma tecnológica segura e acessível em tempo real para atualização do risco. Os elementos do CSP, quando nomeados para um serviço, deveriam ter acesso a uma base de dados, seja qual for, onde pudessem consultar toda a informação relevante. Essa informação seria depois sintetizada no briefing,

mas os elementos poderiam consultá-la antes do serviço e até durante a sua execução. Não ficariam limitados apenas ao que foi transmitido naquele momento inicial.

Por fim, a formação específica nesta área da informação. Atualmente, o foco está muito na vertente técnica e tática do CSP, na segurança pessoal propriamente dita. Mas tudo o que serve de base para aplicar essas técnicas, a informação que sustenta a decisão, acaba por depender bastante da iniciativa e da consideração individual de cada um.

7. Na sua opinião, que tipo de atividades específicas de contrainteligência e contrainformação poderiam ser desenvolvidas ou reforçadas no âmbito do sistema de informações do CSP para potenciar a eficácia da proteção de altas entidades e de outras pessoas que beneficiam de segurança pessoal?

Focando nas situações que dependem diretamente de nós, e tomando como referência a agenda pública e o programa, dou um exemplo: imaginemos uma entidade que vem ao país para um evento estritamente privado e que, nesse contexto, concorda que nada seja divulgado publicamente. Numa situação dessas, considero que deveria existir uma avaliação sistemática das fugas de informação. Ou seja, perceber por que razão determinada informação saiu da nossa esfera. Estou a falar, por exemplo, de itinerários, locais de embarque ou desembarque, meios empenhados ou da própria forma como organizamos o dispositivo. Deve haver uma análise concreta sobre essas fugas e maior atenção a esse tipo de ocorrências.

Não me parece que a solução passe tanto por criar medidas de contrainformação ou desinformação. Se nos focarmos apenas em desenvolver esse tipo de práticas, mas não tivermos controlo sobre as fugas de informação, o resultado pode ser contraproducente. Podemos criar contrainformação e, ao mesmo tempo, essa própria estratégia pode ser exposta como tal, o que é ainda mais grave, sobretudo se isso acontecer dentro do nosso próprio seio.

Podem existir medidas como a compartimentação reforçada da informação em fases críticas da missão ou a realização de simulações de cenários de manipulação mediática de incidentes. No entanto, continuo a achar que investir demasiado em estratégias de contrainformação pode sair-nos "furado" e criar uma imagem pior do que aquela que pretendemos evitar. Em termos práticos, pode ser mais vantajoso não enveredar por esse caminho. A prioridade deveria ser concentrar esforços na prevenção de fugas de informação e na proteção eficaz da informação sensível.

E quando falo em proteger, não significa excluir agentes, chefes ou oficiais do processo. Significa criar mecanismos que garantam que a informação fica devidamente blindada e não

sai do circuito necessário. Se conseguirmos assegurar isso, o problema fica, em grande parte, resolvido por si só, sem necessidade de recorrer a outras medidas mais complexas.

Apêndice H – Entrevista E5

Codificação do entrevistado: E5

Função: Chefe com funções de comando tático num destacamento do CSP

Tempo de experiência numa função ligada ao CSP ou às Informações na PSP: 26 anos

Tempo de serviço na PSP: 34 anos

Entrevistador: Rodrigo Miguel Rosa Rodrigues

Ano: 2026

1. Os polícias do CSP recebem briefings e/ou elementos escritos ou verbais na área da inteligência policial sobre o contexto operacional? Se sim, de que fonte e de que forma?

Aqui talvez possamos dividir a questão em duas situações distintas. Uma coisa é estarmos a trabalhar com uma entidade nacional, por exemplo com o Senhor Primeiro-Ministro, e prepararmos as visitas todas. Fazemos deslocações prévias aos locais, reunimos com quem organiza e com quem convida, no fundo articulamos todo o processo. Chamamos as forças de segurança da área, seja GNR, seja PSP e montamos o programa até o fechar.

Outra realidade é quando estamos no CSP a fazer serviço a entidades estrangeiras. Nesses casos, é-nos atribuído o serviço e é-nos dado apenas o programa da visita da entidade. Eu estive muito tempo nesse tipo de serviço e, na prática, era isso que acontecia, recebíamos o programa da visita e mais nada.

Posso dizer que, em todos os serviços com entidades estrangeiras que fiz, apenas uma vez fui a um briefing na Direção Nacional relacionado com informação de Inteligência propriamente dita. Foi na visita dos Reis da Bélgica e foi a única vez, nos anos em que estive a fazer serviço a entidades estrangeiras, em que tivemos um briefing na DN sobre a ameaça que recaía sobre a família real belga, até porque tinham ocorrido atentados em Bruxelas. De resto, na maioria dos serviços, é apenas um chefe com uma equipa mais pequena, e não é transmitida qualquer informação sobre o porquê de aquela pessoa necessitar de segurança ou se recai alguma ameaça concreta sobre ela.

Falo por mim, eu próprio ia pesquisar à internet para ver se tinha acontecido alguma coisa relevante, porque informação sobre a pessoa em si raramente era recebida.

Posso contar um episódio. Quando estava a distribuir serviço para o Procurador-Geral da Hungria, foi-lhe inicialmente atribuído grau 4, ou seja, praticamente não teria segurança. No entanto, achei estranho virem três elementos de segurança avançada e mais três com o próprio Procurador-Geral. Recebi então um telefonema da embaixada a informar que a equipa de

segurança avançada já estava em Portugal e pretendia reunir. Perguntei se se passava alguma coisa, e disseram-me que ele tinha sofrido um atentado à bomba há dez dias. Fui imediatamente à internet pesquisar o nome do Procurador-Geral da Hungria, e a primeira notícia que apareceu foi precisamente essa, tinha ocorrido um atentado à bomba, com um carro armadilhado que explodiu ao lado do veículo dele quando ia a passar.

Achei estranho que essa informação não tivesse sido considerada desde o início. Tivemos então de alertar para o facto de a pessoa ter sofrido um atentado há dez dias, não há dez meses. Inicialmente tinha grau 4 e, se fosse por isso, nem teria segurança. Naturalmente, a situação foi revista, o grau de ameaça foi alterado e o dispositivo ajustado.

Mas fui eu que pesquisei, e houve também o telefonema da embaixada. Isto demonstra que, na maior parte das vezes, tirando grandes visitas, como aconteceu com os Reis dos Belgas, praticamente não há informação sobre as ameaças que possam recair sobre a pessoa.

Mesmo a nível das entidades nacionais, raramente recebo informação sobre eventuais manifestações. Apenas recebemos diariamente um ficheiro Excel com manifestações previstas, ou seja, aquelas que são comunicadas oficialmente. Mas as inopinadas não constam aí.

Portanto, se a informação circula, tenho a perceção de que não chega a quem está no terreno. Vamos para o terreno e, na prática, somos nós que temos de fazer a pesquisa, porque raramente recebemos informação estruturada sobre isso. É essa a realidade.

2. No âmbito da formação e exercício das funções, os polícias do CSP no terreno são orientados para a recolha de informação como forma de apoio à produção de informações relevantes para a atividade operacional da PSP?

Acho que parte muito da iniciativa de cada um, quando não devia ser assim. Acho que o serviço, ao chegar uma informação, por exemplo, ainda agora vamos ter para a semana vários Chefes de Estado na posse do novo Presidente da República, devia logo tratar dessa parte. Eu sempre tive essa preocupação de ir pesquisar, de tentar conhecer a pessoa, perceber os hábitos e ver se havia alguma coisa relevante. Acho que os meus colegas fazem o mesmo, mas isso devia partir do próprio serviço do DIP ou eventualmente de algum gabinete montado na UEP. Talvez fosse uma boa opção existir na UEP um gabinete que tratasse dessa pesquisa, porque assim poderia começar logo a trabalhar a informação. Neste momento, muitas vezes fica na mão do chefe de equipa que vai apanhar esse serviço ir à internet pesquisar e ver várias coisas.

Eu tive, por exemplo, um caso de um Presidente da República da Eslovénia que todos os dias corria 20 quilómetros. Claro que temos de estar preparados para isso e perceber em que

moldes ele fazia aquilo. Eu fui ver isso à internet. Portanto, muitas dessas informações acabam por vir das pesquisas que fazemos online.

Relativamente à formação, não me recordo de, quando fiz o meu curso haver uma orientação específica nesse sentido. Não sei como está atualmente a formação, se hoje em dia já existe essa orientação. Como digo, eu tive sempre essa iniciativa e acho que os meus colegas fazem o mesmo: ir pesquisar. Quando estava na planificação ou a distribuir serviço, recomendava sempre isso. Porque muitas vezes também não temos uma equipa avançada da própria entidade com quem possamos trocar essas informações e perceber melhor a situação.

Tirando as visitas de Estado dos Presidentes, em que normalmente existe essa estrutura, noutros casos, como ministros ou outras entidades, muitas vezes não há equipa avançada nenhuma. E, nesses casos, não temos contacto direto com a segurança dessa pessoa. Acabamos, portanto, por ser nós próprios a fazer essa pesquisa.

3. Na sua experiência, em operações de segurança pessoal, sente que existem lacunas na partilha de informação entre as subunidades e o CSP e entidades?

No serviço onde estou, nós vamos sempre antes aos locais, temos essa vantagem. Fazemos visitas preparatórias, contactamos a força local e a estrutura local e acabamos por ser nós a fazer essa procura de informação. Portanto, não estamos à espera que a informação venha, seja da DN, seja da UEP. Somos nós que fazemos essa pesquisa no trabalho de preparação das deslocações. Normalmente, como é norma, com cerca de uma semana de antecedência vamos aos locais. Contactamos logo a força local e, se for o caso, também a Câmara Municipal.

Tentamos também colmatar um bocadinho esta questão de as deslocações só serem divulgadas à imprensa muito perto da data. A nota de imprensa a informar sobre uma visita a determinado local só é feita, normalmente, no dia anterior. Claro que, se a visita for à segunda-feira, tem de ser feita na sexta-feira. Isso já dá algum tempo para que, por vezes, aconteçam alguns movimentos inopinados e apareçam pessoas a protestar. Ainda assim, tentamos colmatar um pouco essa situação. Foi até falado com o gabinete de imprensa no sentido de se divulgar sempre apenas na véspera, para não dar muito tempo a quem queira organizar alguma ação inesperada.

Depois, fazemos também a pesquisa através da força de segurança local. Eles ficam mais atentos e também fazem a sua própria pesquisa para perceber se pode acontecer alguma coisa. Portanto, acabamos por trabalhar muito desta forma.

4. Do ponto de vista da proteção de altas entidades, considera que atualmente existem (ou não) práticas estruturadas de contrainteligência e/ou contrainformação no CSP?

Se existe, eu desconheço. Como eu digo, a informação que chega ao CSP é muito limitada. Percebemos que há a visita de uma alta entidade, neste caso, por exemplo, uma alta entidade estrangeira, mas a informação que nos chega, muitas vezes, resume-se praticamente ao programa da visita. Para além disso, normalmente não vem mais informação nenhuma.

Não chega muita informação adicional relativamente a eventuais ameaças ou a esse tipo de enquadramento. Pelo menos, eu não tenho conhecimento de que isso seja transmitido de forma regular.

5. Se existisse uma componente de inteligência policial especificamente dedicada a apoiar o CSP, que prioridades operacionais e táticas deveria ter?

Aqui nós temos uma plataforma partilhada de operações de segurança. Antigamente, estas coisas faziam-se por fax ou por e-mail, mas hoje existe essa plataforma. No entanto, nem toda a gente tem acesso a ela e só é possível aceder através dos computadores oficiais por questões de segurança.

Essa plataforma funciona muito bem. Acho que é uma ferramenta muito útil porque facilita bastante o nosso trabalho. E teria capacidade, ou então poderia criar-se algo semelhante, para também integrar este tipo de informação. Dentro da própria plataforma poderiam criar uma pasta ou um espaço específico, porque aquilo permite organizar vários tipos de conteúdos.

O Gabinete de Informações, ou o DIP, também é notificado da visita das entidades, mesmo no caso das nossas entidades nacionais. Por exemplo, quando o Senhor Primeiro-Ministro vai viajar ou deslocar-se, é criado um relatório, aquilo que se chama um relatório de deslocação e depois a DN faz os despachos. Esse despacho segue em conhecimento para o CSP. No entanto, nunca vi ser acrescentada ali informação adicional desse tipo. Por isso, acho que esta plataforma podia ser utilizada também para esse efeito. Podia fazer-se uma pesquisa e colocar lá informação relevante. Hoje em dia é uma ferramenta muito útil e podia perfeitamente ser aproveitada também para isso.

6. Que alterações considera essenciais para que as informações circulem de forma mais eficaz entre quem produz inteligência policial e quem comanda ou executa operações de segurança pessoal e entre estes e as Unidades Policiais territorialmente competentes?

Tudo o que venha a contribuir para o melhor desenrolar da operação, seja a coordenação com a força local, desde um pedido de estacionamento para a partida, a juntar, se houver informação de algum tipo de protesto, por exemplo, que possa haver, ou de algum tipo de manifestação que se esteja a organizar, isso tudo vai contribuir para que as coisas corram melhor.

Nós agora tivemos um episódio. Apareceram uns senhores, inopinadamente, com cartazes da Casa dos Direitos dos Animais. Eles não informaram que iam lá. Detetámos depois ali no exterior, junto à Câmara Municipal. Tivemos de tomar ali outras medidas para a saída, ver se não passávamos junto aos senhores. Não foi detetado antes, mas às vezes há trocas de mensagens e isso às vezes chega-nos essa informação. Muitas vezes por grupos de WhatsApp, fazem essas coisas e acabam por chegar. Portanto, se houver e nos derem essa informação atempadamente, claro que no fim as coisas vão correr melhor, porque dá para a gente prevenir antes de chegar a um sítio.

Claro que nós aqui temos sempre uma equipa avançada. O local onde o senhor primeiro vai é visto primeiro. É evidente que, se isso estiver lá a acontecer, quem lá está no local avisa logo, tenta ver aí com o senhor Primeiro-Ministro. Mas temos entidades nacionais, por exemplo, a nível de ministros, em que os nossos ministros têm segurança, mas não têm uma equipa avançada e esses precisam ainda de mais informação.

Nós temos sempre esta vantagem de ter equipa avançada. Se alguma coisa estiver ali a acontecer, somos logo informados. Mas a maioria não tem. Portanto, isso, parecendo que não, quer para nós quer para a força local, seria bastante útil haver essa partilha e essa maior contribuição sobre esses assuntos, sobre essa matéria, que é coisa que eu não vejo que haja assim muito.

7. Na sua opinião, que tipo de atividades específicas de contrainteligência e contrainformação poderiam ser desenvolvidas ou reforçadas no âmbito do sistema de informações do CSP para potenciar a eficácia da proteção de altas entidades e de outras pessoas que beneficiam de segurança pessoal?

Pois, aqui não sei como é que se poderia fazer. Nós tentamos não alertar muito antes a ida da entidade. Tentamos jogar um bocadinho aqui com a questão de quando é que se anuncia à imprensa. A contra-informação aqui não sei de que modo é que se poderia fazer, porque se o Senhor Ministro vai a Évora, não podemos dizer que vai a Beja.

Portanto, jogamos um bocadinho com o dar a conhecer o mais próximo possível, na véspera, e não às vezes com cinco dias de antecedência ou uma semana de antecedência. Isso também é combinado com quem está a organizar, seja a Câmara Municipal, seja uma universidade, ou seja uma fábrica que se vá visitar, porque o anfitrião também vai divulgar. E isso é combinado com o gabinete de imprensa para só ser divulgado naquela data. Podem fazer os dois até ao mesmo tempo e o mínimo mais perto da data da visita.

A contrainformação aqui não estou a ver como é que poderia funcionar, é complicado nessa parte. Bem, os trajetos nós não divulgamos, como é óbvio. Agora, acho um bocado complicado a contrainformação funcionar para este tipo de situações, porque é o que eu digo, não podemos dizer à comunicação social que a entidade vai a um sítio e afinal vai a outro.

Apêndice I – Entrevista E6

Codificação do entrevistado: E6

Função: Chefe com funções de comando tático num destacamento do CSP

Tempo de experiência numa função ligada ao CSP ou às Informações na PSP: 26 anos

Tempo de serviço na PSP: 35 anos

Entrevistador: Rodrigo Miguel Rosa Rodrigues

Ano: 2026

1. Os polícias do CSP recebem briefings e/ou elementos escritos ou verbais na área da inteligência policial sobre o contexto operacional? Se sim, de que fonte e de que forma?

É assim, isto depende sempre do grau de ameaça que é atribuído à entidade e à pessoa proteger. Se o grau for reduzido, isso é executar o serviço de acordo, porque há muitos serviços que nem têm grau de ameaça e é só por inerência do cargo que a entidade em causa exerce. Quando o grau é significativo, ou seja, se é grau 3, a partir daí, já há um briefing e é o SIS que difunde através do SSI se há alguma ameaça relevante e tendo em conta os pontos do trajeto que a entidade segue, se há alguém que pode causar perigo.

2. No âmbito da formação e exercício das funções, os polícias do CSP no terreno são orientados para a recolha de informação como forma de apoio à produção de informações relevantes para a atividade operacional da PSP?

A missão é conduzida sempre tendo em conta o grau de ameaça. E depois, tendo em conta o grau de ameaça, se o grau de ameaça é significativo, que é o grau 3. A partir daí faz-se recurso a Fontes Abertas, é contactada a força policial territorialmente competente, assim como o SIS através do SSI.

Isto porque no terreno existe sempre um reconhecimento antes através de uma equipa de segurança avançada que irá tentar saber junto da força policial territorialmente competente, se há algum alguma hostilidade em termos de manifestações ou outros eventos desse tipo. Se existe, por exemplo, em visitas a empresas algum burburinho em termos de mau estar dos trabalhadores, pois isso tudo pesa para o bom funcionamento da missão. Porque se houver problemas dentro ou problemas laborais, nós já vamos ter que tentar contactar a Comissão de trabalhadores para ver o que é que se passa ali e se há ali uma hostilidade.

3. Na sua experiência, em operações de segurança pessoal, sente que existem lacunas na partilha de informação entre as subunidades e o CSP e entidades?

Sim, isso acontece. Quando vamos, principalmente para a área da GNR. Por vezes, não somo muito bem recebidos entre aspas porque que eles acabam por resguardar um bocadinho a informação. Isto porque querem ser eles a passarem essa informação às equipas próprias deles ao nível da investigação criminal. Por isso é que às vezes eles querem em visitas a locais, na área da GNR, eles querem pôr sempre uma equipa do de investigação criminal pois afirmam que eles é que conhecem terreno e depois acabam por não passar a informação. Aliás há exemplos como o Euro 2004, em que foram notórios vários problemas com a GNR, porque eles não passavam informação e faziam muito "finca-pé" mesmo para, por exemplo, em termos dos hotéis, na segurança dos perímetros dos hotéis onde estavam as seleções ou grave graves problemas com eles. Aliás, às vezes ou quase a chegar a vias de facto, por causa dessa situação, deles esconderem informação e não querem partilhar da mesma forma.

Também há, às vezes, com a PJ também certas situações de proteção de testemunhas, a PJ também não, não difunde tudo o que sabe. Eles resguardam-se no segredo de justiça e depois quando nós vamos para proteger a testemunha, nós temos que saber tudo o que se passa, o que é que está por trás, o inquérito…. Temos de saber o que é que está por trás, Tudo! Para a boa missão e para a nossa proteção, não apenas da testemunha, mas a nossa, principalmente. Às vezes a informação é sonegada e nós só depois é que vamos sabendo pela própria testemunha nos casos de testemunhas de processos complicados, elas é que nos acabam por "abrir o jogo".

Comigo aconteceu também com a PSP, com pessoal da DIC. Eles acabam por não partilhar alguma informação que viemos a perceber na altura que tinha sido crucial para nós e para a boa execução do Serviço.

Isto acontece porque, nós às vezes chegamos ao terreno e eles não sabem. Há alturas em que sabem tudo e até sabem mais que nós e há outras em que não sabem nada. Aliás, ultimamente, por exemplo, no mandato do António Costa, aqui na zona norte eu e o outro colega é que fazíamos praticamente tudo, ao nível de preparatórias, sendo que o gabinete só difundia informação na véspera. Tanto a GNR como a PSP não gostavam muito de nomeadamente dos comandantes da área, não gostava muito de não saber. Sendo, muitas vezes o próprio comandante CSP a falar diretamente com os comandantes, porque eles não tinham que saber mais que nós.

Depois também há outro problema que surge, nomeadamente na PSP, e eu falo no comando do Porto. Aquando da chegada de uma entidade difundem pelas divisões todas ao

invés de ser só para aquela divisão da área e para o comandante de esquadra, aquilo acaba por chegar a toda a gente e toda a gente fica a saber pormenores específicos da missão. Essas coisas não podem acontecer, isto põe em risco a missão. Em manifestações, quando as situações estão críticas, os manifestantes apercebem-se com a presença dos policias, mas quando a presença é mais discreta eles já não sabem. Isso é algo muito complicado de gerir.

4. Do ponto de vista da proteção de altas entidades, considera que atualmente existem (ou não) práticas estruturadas de contrainteligência e/ou contrainformação no CSP?

Não, eu penso que não, isso nós não utilizamos muito. Talvez tenha sido utilizado na altura do ex-Presidente Cavaco Silva. Ultimamente, não, essa prática de estar a difundir uma informação contrária? Não, não tenho assim muito conhecimento disso.

5. Se existisse uma componente de inteligência policial especificamente dedicada a apoiar o CSP, que prioridades operacionais e táticas deveria ter?

É assim primeiro, eu acho que o CSP devia ter deveria ter equipas de informação de informação só a trabalhar para o CSP. Isto porque nós, em termos de missões, que se pede informação, aquilo demora muito tempo a chegar muito tempo e às vezes já chega fora do prazo. O CSP deveria ter para cada missão, sobretudo missões de risco elevado, equipas que avançavam à frente a recolher informação para depois para canalizar para a equipa de segurança que está com a entidade. Só assim é que se consegue levar uma missão a cabo cabalmente, porque não havendo informação, corremos o risco de ser surpreendidos. Mesmo com uma ou duas equipas avançadas, se não tiveres uma informação prévia do que vai acontecer para acautelar as situações e programar os serviços, a missão pode não correr bem. Por isso é fundamental ter equipas de informações a trabalhar, tenda já esta sido umas das prioridades de alguns comandantes do CSP. Porque isso é fundamental, ter uma equipa avançada com informações é fundamental!

Aliás em missões com presidentes estrangeiros, eles vêm muito à frente. Por exemplo, quando veio cá o Fidel Castro, nós fizemos um levantamento na Ribeira do Porto, de todas as pessoas que viviam de frente e nas traseiras do edifício da alfândega. E viemos a descobrir lá um casal de cubanos que estavam lá há 1 ano a recolher informação sobre a visita do Fidel Castro.

6. Que alterações considera essenciais para que as informações circulem de forma mais eficaz entre quem produz inteligência policial e quem comanda ou executa operações de segurança pessoal e entre estes e as Unidades Policiais territorialmente competentes?

Primeiramente, o Canal tem que ser restrito, não pode ser um canal aberto. Tem que ser difundido através da chefia e para quem efetivamente precisa da informação, segundo o princípio da necessidade de informação. Porque estar a difundir essa informação para toda o efetivo de uma esquadra, por exemplo, é péssimo para o serviço. E, portanto, criar o que estávamos a falar, criar equipas de informações e depois haver uma ligação mesmo com as outras polícias e com o SIS. Já existe um elo de ligação através do oficial que está no SSI já existe, mas às vezes isso não é suficiente. Deveria haver ali uma parte onde se conseguisse chegar mais rapidamente à informação, porque CSP necessita de informação imediata, não é informação a posteriori.

7. Na sua opinião, que tipo de atividades específicas de contrainteligência e contrainformação poderiam ser desenvolvidas ou reforçadas no âmbito do sistema de informações do CSP para potenciar a eficácia da proteção de altas entidades e de outras pessoas que beneficiam de segurança pessoal?

Eu penso que aqui a questão da contra informação faria mais sentido ser usada na parte da proteção de testemunhas. Isto porque em termos de uma visita de Chefe de Estado estrangeiro, os gabinetes difundem sempre com 12 ou 24 horas de antecedência a agenda para a comunicação social. Estar a fazer prática de contra informação iria criar um problema com os OCS, e, acima de tudo, as altas entidades que têm segurança pessoal querem é dar-se bem com a comunicação social.

Estou-me a lembrar agora quando veio cá um jornalista italiano, que corria muitos riscos por ser muito polémico, aí sim faz todo o sentido haver uma contra informação. Agora, em termos de segurança pessoal de altas entidades e pronto não sei até que ponto faz sentido para nós.

Estou-me a lembrar de vários casos, nomeadamente africanos e com regimes ditatoriais, como do Hugo Chávez e outros em que com eles funciona a contra informação, eles dizem que chegam às 2 da manhã, e depois só chegam no outro dia às 2 da tarde. Pronto, agora em termos das altas entidades típicas nossas e no espaço europeu, mais no espaço europeu, não estou a ver como a contra informação aí seja relevante.

Apêndice J – Entrevista E7

Codificação do entrevistado: E7

Função: Chefe com funções de comando num grupo operacional do CSP

Tempo de experiência numa função ligada ao CSP ou às Informações na PSP: 19 anos

Tempo de serviço na PSP: 28 anos

Entrevistador: Rodrigo Miguel Rosa Rodrigues

Ano: 2026

1. Os polícias do CSP recebem briefings e/ou elementos escritos ou verbais na área da inteligência policial sobre o contexto operacional? Se sim, de que fonte e de que forma?

É assim, nós não sabemos tanto quanto gostaríamos e quanto deveríamos saber. Em situações normais de visitas, isso não acontece. Não recebemos informação adicional, a não ser que exista algum caso excecional. Aí, sim, é-nos transmitida informação.

Mas essa informação é enviada de forma puramente formal. Temos conhecimento através do e-mail institucional, onde recebemos o relatório do DIP ou do Núcleo de Informações do COMETLIS.

Em serviços de maior envergadura, sim, já é hábito ser-nos transmitida informação relevante sempre que existe alguma situação que devamos conhecer previamente.

Relativamente ao conteúdo desses relatórios do DIP, por exemplo, se houver previsão de manifestação, existindo identificação de manifestantes ou referência a possíveis ativistas, isso é informado. Basicamente, indicam-nos o que podemos esperar e o que eventualmente não devemos esperar, em termos de enquadramento da situação.

2. No âmbito da formação e exercício das funções, os polícias do CSP no terreno são orientados para a recolha de informação como forma de apoio à produção de informações relevantes para a atividade operacional da PSP?

Sim, no curso isso é ministrado. Há uma altura em que existe um módulo do curso em que o DIP vem dar formação nesse sentido e nós somos orientados para esse tipo de recolha e alertados para aquilo que devemos fazer em fontes abertas.

No decurso do serviço, por vezes isso é relembrado. Eu utilizo isso. Depois, espero também que, face ao trabalho que é desenvolvido, nomeadamente pelo próprio SIS, se houver algum alerta que nós devamos ter conhecimento, sejamos informados disso.

Agora, não fazemos isso diariamente, porque a partir do momento em que isso é ministrado no curso técnico, cada um sabe aquilo que tem de fazer relativamente a fontes abertas. Eu, quando vou para uma missão, quando me é atribuída uma missão, vou logo fazer pesquisa em fontes abertas. Procuro saber sobre a entidade, se há algum tipo de ameaça, se já foi vítima de algum ataque ou não. Faço todo esse tipo de pesquisa em fontes abertas, na internet.

3. Na sua experiência, em operações de segurança pessoal, sente que existem lacunas na partilha de informação entre as subunidades e o CSP e entidades?

Sim, no caso do CSP, dentro das unidades operacionais, nós pertencemos todos à UEP, pelo que aí não existe essa problemática. Quando as outras subunidades são empenhadas em missões de apoio à segurança pessoal, existe essa colaboração e há sempre ligação entre as partes. Portanto, a informação flui com rapidez.

Agora, relativamente a outras entidades, já não é bem assim. Aí devia haver uma maior ligação. Obviamente que, em determinados eventos e com determinado tipo de entidades, existe sempre um ponto de contacto para fazer essa articulação, e nesses casos é possível haver uma colaboração mais estreita, nomeadamente também com o DIP. Mas nas missões do dia a dia, isso não acontece.

4. Do ponto de vista da proteção de altas entidades, considera que atualmente existem (ou não) práticas estruturadas de contrainteligência e/ou contrainformação no CSP?

Enfim, no CSP não temos um núcleo de informações. O CSP não possui uma estrutura própria de informações.

Nós trabalhamos com aquilo que o DIP nos transmite, com as avaliações que eles fazem. Também temos o núcleo de operações e informações da UEP, sendo que eles recebem essas informações por parte do DIP e depois canalizam para nós.

Relativamente à contrainformação e à desinformação, nós fazemos isso, no fundo, através de fontes abertas e por iniciativa própria, mantendo-nos atualizados. Durante o curso também nos é ministrada formação no sentido de fazermos contravigilâncias. Procuramos não ter sempre a mesma rotina.

Temos também de estar atentos a diversos tipos de campanhas de desinformação que possam existir. Por vezes consultamos a internet para verificar se existe algum caso ou alguma situação desse tipo.

5. Se existisse uma componente de inteligência policial especificamente dedicada a apoiar o CSP, que prioridades operacionais e táticas deveria ter?

Sim, o que eu acho é que nós devemos trabalhar, e a segurança pessoal deve trabalhar, sobretudo na prevenção. Eu diria que o mais importante é a prevenção.

Como é que fazemos isso? Através da monitorização de fontes abertas: redes sociais, notícias, tudo aquilo que exista disponível. Devemos detetar discursos relativamente a uma entidade que possam ser hostis. Identificando a pessoa, devemos acompanhar esse discurso, perceber se ele é continuado. Devemos procurar indivíduos que estejam radicalizados e que tenham um discurso contra determinada entidade.

Se tivermos de reagir é porque alguma coisa já correu mal antes de chegarmos aí. Por isso, acho que devemos trabalhar bastante na área da prevenção e, para isso, temos de identificar precocemente as ameaças.

Além disso, devemos analisar o comportamento de determinado tipo de indivíduos, tendo em conta o discurso que têm, para perceber se existe algum risco de poderem passar das palavras aos atos.

Devemos verificar se há tentativas de aproximação às entidades, se existe algum tipo de sinal de obsessão com determinadas entidades.

Devemos também prevenir fugas de informação.

Atualmente, aquilo que também temos de considerar muito é a vertente cibernética. Acho que o futuro passa muito por tudo o que seja ciber, engenharia social e ataques informáticos para exploração de dados. Esse é um desafio bastante grande que a Polícia vai atravessar nos próximos anos, e o CSP obviamente também. Portanto, temos de tentar contornar essa situação e evoluir nesse sentido.

6. Que alterações considera essenciais para que as informações circulem de forma mais eficaz entre quem produz inteligência policial e quem comanda ou executa operações de segurança pessoal e entre estes e as Unidades Policiais territorialmente competentes?

Sim, eu acho que há necessidade de a inteligência policial estar diretamente a trabalhar connosco na parte operacional, integrada mesmo nas equipas, porque nós precisamos de informação em tempo útil, no momento. E para isso é preciso ter sempre alguém da área das informações a trabalhar connosco. Neste momento, essa componente está dependente do DIP, que tem de dar resposta a toda a Polícia, portanto não se pode focar apenas no CSP. E o CSP

não pode estar à espera que as situações se resolvam ou que a informação chegue quando for possível. Eu acho que nós devíamos, se calhar, ter um núcleo próprio para responder às nossas necessidades.

Quanto à ligação territorial, com as unidades de polícia territorialmente competentes, eu penso que essa ligação acaba por existir. Não tanto com a parte da inteligência ou das informações, porque isso acontece basicamente em grandes eventos. A questão é que, quando estão no terreno ou quando há alguma entidade que tenha algum tipo de ameaça, eles estão no terreno e há essa ligação connosco.

A ligação territorial acaba por ser feita e acaba por fluir. Porque eu, quando vou a qualquer tipo de evento, tenho sempre contacto com a polícia territorialmente competente. Se estou numa entidade, por exemplo da área da Defesa, Justiça ou outra entidade com determinado tipo de local próprio, faço sempre contacto com a entidade territorial competente, alerto para as minhas necessidades e digo aquilo que preciso. Portanto, essa ligação acaba por ser feita. Em grandes eventos existe o posto de comando tático, onde está um representante de cada valência.

O que poderíamos fazer para melhorar isto? Talvez alterações tecnológicas na partilha de informação. Se calhar criar uma plataforma digital onde eu possa ter acesso à informação de forma rápida, sem comprometer a segurança da informação. Mas isso implica investimento. Tem de haver investimento nessas plataformas digitais.

7. Na sua opinião, que tipo de atividades específicas de contrainteligência e contrainformação poderiam ser desenvolvidas ou reforçadas no âmbito do sistema de informações do CSP para potenciar a eficácia da proteção de altas entidades e de outras pessoas que beneficiam de segurança pessoal?

A contrainformação inclui a monitorização de ameaças, a identificação de indivíduos, a proteção de itinerários e agendas. Tem de haver proteção e temos de procurar detetar fugas de informação. Temos também de verificar se podem existir fugas internas que comprometam a missão. Temos de estar atentos à atividade cibernética, tendo em conta que trabalhamos cada vez mais no digital. Os equipamentos que utilizamos têm de estar protegidos, porque hoje em dia trabalhamos com computadores, telemóveis e tablets, e toda a informação sensível passa por esses equipamentos. É natural que os atacantes tentem aceder a esses dispositivos para extrair informação, e nós temos de investir nisso. Temos de investir em cibersegurança, na

encriptação de dispositivos e na encriptação das comunicações. Temos de antecipar tudo isso para que não sejamos expostos.

Por vezes, pode ser necessário utilizar desinformação para criar confusão em potenciais ameaças. Se houver determinado tipo de missões em que se veja essa necessidade, pode fazer sentido divulgar alguma informação para criar confusão e reduzir a nossa previsibilidade.

Neste momento, uma das maiores ameaças com que nos deparamos é a cibersegurança. Temos de evoluir nessa área. E, por exemplo, os drones são atualmente uma das maiores ameaças para a segurança pessoal.