

INSTITUTO DE ESTUDOS SUPERIORES MILITARES
CURSO DE ESTADO-MAIOR CONJUNTO

2012/2013



TII

ANÁLISE CRIMINAL E SISTEMAS DE INFORMAÇÃO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOCTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS E DA GUARDA NACIONAL REPUBLICANA.



INSTITUTO DE ESTUDOS SUPERIORES MILITARES

ANÁLISE CRIMINAL E SISTEMAS DE INFORMAÇÃO

Major de Inf.^a da GNR Carlos Alexandre Quatorze Pereira

Trabalho de Investigação Individual do CEM-C 2012/13

Pedrouços – 2013



INSTITUTO DE ESTUDOS SUPERIORES MILITARES

ANÁLISE CRIMINAL E SISTEMAS DE INFORMAÇÃO

Major de Inf.^a da GNR Carlos Alexandre Quatorze Pereira

Trabalho de Investigação Individual do CEM-C 2012/13

Orientador: Coronel de Inf.^a da GNR Raul Maia Pires

Pedrouços – 2013



Agradecimentos

O CEM C é um período “particular” no percurso de um Oficial Superior, não apenas pela elevada intensidade, mas também pela oportunidade que proporciona de diversificar experiências, conhecimentos e pelo contacto com realidades diversas. Para mim foi sobretudo “especial” pela camaradagem que senti “ao longo do caminho íngreme”. A todos os camaradas com tive o privilégio de partilhar este “trajeto” agradeço o apoio, os debates, bem como os saberes e experiências permutados, que muito me enriqueceram.

A elaboração do presente TII não teria sido possível, ou não teria tido a mesma objetividade, sem a prestimosa colaboração de algumas personalidades que gostaria de destacar e citar, com um singelo agradecimento.

A todos os que aceitaram partilhar os seus sólidos conhecimentos em proveitosas entrevistas. Aos Oficiais da GNR: Coronel João Borges, Coronel Albano Pereira, Coronel Ócar Rocha, Ten. Cor. Joaquim Grenho, Ten. Cor. Carreirinha Branco, Ten. Cor. Nascimento, Ten. Cor. Altide Cruz, Major Paulo Santos. Aos Oficiais da PSP: SubIntendente Alexandre Vieira e Comissário Tito Fernandes. Ao Inspetor Paulo Gomes, da PJ e ao Inspetor Adjunto Principal Fernando Marques, do SEF.

Aos camaradas Lima Letras e Vitor Assunção pela amizade, apoio e incentivo que sempre demonstraram ao longo do tempo. A disponibilidade e empenho que demonstraram, em especial na fase revisão deste trabalho, foram fundamentais para a sua concretização.

Um agradecimento especial ao Coronel Maia Pires pela forma dedicada e lúcida como me orientou e motivou para a execução do presente trabalho.

À Daniela, pelo tempo que deixei de lhe dedicar enquanto crescia, e à Paula, por tudo...



Índice

Introdução	1
1. As Informações- Enquadramento Conceptual	7
a. Das <i>Informações</i> Estratégicas e de Segurança às <i>Informações</i> Policiais	7
b. As <i>Informações</i> Policiais	9
c. O Policiamento Guiado por Informações (<i>Intelligence Led Policing</i>).....	15
2. Análise Criminal.....	19
a. Definição e caracterização	20
b. Análise Estratégica e Análise Operacional	21
c. A função do Analista Criminal.....	23
3. Sistemas de Informação - Enquadramento concetual.....	26
a. Os Sistemas de Informação	26
b. As Tecnologias de Informação (TI)	27
4. Sistemas de Informação Policiais	29
a. Análise evolutiva em Portugal	29
b. Os Sistemas de Informação Policiais em Portugal	31
c. A adequação dos SI à AC.....	32
d. A Interoperabilidade entre SI e a patilha de Informação Criminal	34
e. A Plataforma Para o Intercâmbio de Informação Criminal PIIC	34
f. Perspetivas de evolução dos SI	35
Conclusões	38
a. Resposta às questões derivadas.....	39
b. Teste das Hipóteses	41
c. Resposta à questão central.....	43
Bibliografia.....	46
Apêndice 1 - Linha de Orientação Metodológica	AP-1-1
Apêndice2 – Corpo de Conceitos.....	AP-2-1
Apêndice 3 – Trabalho de Campo.....	AP-3-1
Apêndice 3 – Caracterização dos SI das FFSS	AP-4-1
Apêndice 4 – Ciclo de produção de Informações.....	AP-5-1
Índice de Figuras	
Figura 1 – Classificação das Informações Policiais	10
Figura 2 – Diagrama das Informações como produto.....	12
Figura 3 – <i>Intelligence Led Policing</i> – Modelo dos 3I.....	17
Figura 4 – Diagrama do Ciclo de Produção de Informações	AP -4-1



Resumo

O presente trabalho, realizado no âmbito do Curso de Estado Maior Conjunto, visa estudar a atividade da Análise Criminal, nas suas diversas perspetivas (estratégica e operacional), enquanto parte essencial do Ciclo de Produção de Informações, evidenciando o contributo para o processo de decisão policial, suportada pelos mecanismos essenciais dos Sistemas de Informação policiais.

O nosso objetivo central consiste na apresentação de um estudo que contribua para a compreensão da importância das Informações Policiais, em geral, e da Análise Criminal, em particular, na prevenção e combate aos fenómenos criminais em Portugal, face aos Sistemas de Informação policiais implementados nas Forças e Serviços de Segurança, visando avaliar a sua interoperabilidade, coordenação e partilha de informação.

O enfoque para o estudo centrou-se na avaliação dos diferentes Sistemas, procurando verificar as suas linhas de força e debilidades face às necessidades do trabalho dos analistas criminais nessas organizações, em linha com os princípios do denominado *Intelligence Led Policing*.

Concluimos que existem lacunas importantes ao nível dos sistemas de informação implementados, não apenas nas plataformas tecnológicas, mas também ao nível da qualidade dos dados, da interoperabilidade entre sistemas, bem como na formação dos analistas e dos elementos policiais em geral, com impactos contraproducentes na qualidade dos produtos resultantes da análise criminal e ao nível do apoio à decisão, em Portugal.

As conclusões extraídas permitirão, certamente, reflexões em torno das matérias mencionadas, abrindo novos horizontes numa lógica de agilizar a resposta das Instituições policiais Portuguesas às problemáticas criminais emergentes.



Abstract

The present study, elaborated in the context of the Portuguese Staff College Course, intends to analyse the Criminal Analysis, taking into consideration its different levels (strategic and operational), as part of the Intelligence Cycle, contributing to the police decision making process, always supported by effective police information systems.

Our main objective is to elaborate a study capable to contribute to the comprehension of the police intelligence process, in general, and the criminal analysis, in particular, taking into account the prevention and disruption of the criminal phenomena in Portugal, with the essential contribution of the diverse police corps information systems, envisioning the evaluation of the interoperability, coordination and information sharing capacity

The investigation was centred on the assessment of the diverse systems, looking for its strengths and weakness concerning the criminal analyst's needs within those Organisations and in line with Intelligence Led Policing doctrine and principles .

The studied results allowed comprehending the existent gaps on the police information systems, not only at a technological level but also concerning the data quality, the systems interoperability, as well as with the analysts and other policeman level of training with a negative impact on the quality of the criminal analysis products and consequent decision support.

The obtained conclusions constitute a contribution for the debate and critical thinking related to the studied subject, thus opening new perspectives in a rational of creating improved responses to the emergent criminal problematic.



Palavras- Chave

Análise Criminal; Sistemas de Informação; Informações Policiais; Investigação Criminal; Forças e Serviços de Segurança



Lista de abreviaturas

AC	Análise Criminal
ACC	<i>Australian Crime Commission</i>
ACRI	Arquivo Central do Registo de Informações
ADV	Adversário
AFP	<i>Australian Federal Police</i>
AI	Abertura de Investigação
AJ	Autoridades Judiciárias
ASAE	Autoridade de Segurança de Atividades Económicas
AWF	<i>Analist Working Files</i>
BD	Bases de Dados
CEMC	Curso de Estado-maior Conjunto
CISC	<i>Criminal Intelligence Service Canada</i>
CNPD	Comissão Nacional de Proteção de Dados
COMINT	<i>Signals Intelligence</i>
CPI	Ciclo de Produção de Informações
CPP	Código do Processo Penal
CRP	Constituição da Republica Portuguesa
DGSP	Direção Geral dos serviços Prisionais
DIC	Direção de Investigação Criminal
DIP	Departamento de Informações Policiais
EUA	Estados Unidos da América
FFSS	Forças e Serviços de Segurança
FS	Forças de Segurança
GCS	Gabinete Coordenador de Segurança
GNR	Guarda Nacional Republicana
H	Hipótese
HUMINT	<i>Human Intelligence</i>
IC	Investigação Criminal
IESM	Instituto de Estudos Superiores Militares
ILP	<i>Intelligence Led Policing</i>
ILP	Policiamento Guiado por Informações (<i>Intelligence Led Policing</i>)
IMINT	<i>Imagery Intelligence</i>
IP	Informações Policiais



IPRI	Instituto Português de Relações Internacionais
LO	Lei Orgânica
LOIC	Lei Orgânica da Investigação Criminal
LSI	Lei de Segurança Interna
MAI	Ministro da Administração Interna
MDN	Ministro da Defesa Nacional
MJ	Ministério da Justiça
MO	<i>Modus Operandi</i> ou <i>Modi Operandi</i> (plural)
MP	Ministério Público
NCIS	<i>National Criminal Intelligence Service</i>
NIM	<i>National Intelligence Model</i>
NRATI	Núcleo regional de arquivo e tratamento de informação
NRBQ	Nuclear, radiológico, biológico e químico
OCS	Órgãos de comunicação social
OI	Organizações Internacionais
OPC	Órgãos de Polícia Criminal
OSINT	<i>Open Source Intelligence</i>
PCCCOFSS	Plano de Coordenação, Controlo e Comando Operacional das Forças e
PESI	Plano Estratégico de Sistemas de Informação
PIIC	Plataforma para o Intercâmbio de Informação Criminal
PJ	Polícia Judiciária
PP	Pergunta de Partida
Projeto PIC	Projeto de Partilha de Informação Criminal
PSP	Polícia de Segurança Pública
QC	Questão Central
QD	Questões Derivadas
RADINT	<i>Radar Intelligence</i>
RASI	Relatório Anual de Segurança Interna
RU	Reino Unido
SAPIC	Sistema de Apoio à Prevenção e Investigação Criminal
SEF	Serviço de Estrangeiros e Fronteiras
SEI	Sistema Estratégico de Informação
SG SEPNA	Sistema de Gestão do Serviço de Proteção da Natureza e Ambiente
SG SSI	Secretário-geral do Sistema de Segurança Interna
SGBD	Sistemas Gestor de Bases de Dados



SGO	Sistema Gestão Operacional
SGR	Sistema de Gestão Rodoviária
SI	Sistemas de Informação
SICOP	Sistema de Coordenação Operacional
SIED	Serviço de Informações Estratégicas de Defesa
SIG	Sistema de Informação Geográfica
SII	Sistema Integrado de Informação
SIIC	Sistema Integrado de Informação Criminal
SIIOP	Sistema Integrado de Informações Policiais e Operacionais
SIPEP	Sistema de Informação do Passaporte Eletrónico Português
SIRESP	Sistema Integrado das Redes de Emergência e Segurança em Portugal
SIRP	Sistema de Informações da Republica Portuguesa
SIS	Serviço de Informações de Segurança
SIVICC	Sistema de Vigilância, Comando e Controlo da Costa Portuguesa
SOCA	<i>Serious and Organised Crime Agency</i>
SSI	Sistema de Segurança Interna
TI	Tecnologias de Informação
TN	Território Nacional
UCAT	Unidade de Coordenação Antiterrorismo



Introdução

Introdução ao tema e definição do contexto da investigação

As sociedades hodiernas encontram-se sujeitas a mudanças rápidas, quer do ponto de vista económico quer social, geradas por diversos fatores onde podemos incluir, a globalização, a ausência de fronteiras físicas, a melhoria das vias de comunicação, o progresso tecnológico, com acelerada informatização e processamento em rede que suporta grande parte das atividades humanas, sendo facilitadoras de fenómenos de criminalidade cada vez mais complexos, facilitando a transnacionalidade e o aprimorar dos “*modi operandi*” (MO) por parte de grupos criminais.

Estas alterações dos padrões criminais tornam inevitável a procura por parte das Instituições estatais de novos caminhos, que lhes possibilitem adaptar-se para os enfrentar, gerando, forçosamente, mudanças ao nível do trabalho policial, judicial e político, na implementação de políticas sociais adequadas.

O conhecimento é fundamental para guiar estes novos caminhos de mudança institucional na prevenção e no combate ao crime. É crucial conhecer a realidade dos fenómenos criminais, as suas causas e consequências, os seus autores, os meios que possuem e a forma como atuam nas suas atividades, bem como a incidência temporal e geográfica da sua atuação.

Reportando-nos especificamente ao ambiente policial, poderemos caracterizá-lo como de extrema complexidade, pelo incontável número de fatores, internos e externos, que o influenciam e condicionam, aos diversos níveis: tático; operacional e estratégico. As ameaças, os riscos e os perigos não têm fronteiras, pelo que os limites à ação das Forças e Serviços de Segurança (FFSS) estão em constante redefinição e ajustamento às novas exigências de liberdade e segurança dos cidadãos (Guedes, 2009 cit. (Elias, 2012, p. 5).

As FFSS, para estarem habilitadas a lidar com o meio complexo onde atuam, devem basear a atuação dos seus elementos numa adequada gestão da informação, passando não apenas pela pesquisa, análise e tratamento da informação disponível, mas também pela sua disponibilização aos elementos que dela realmente necessitam tempestivamente. É neste contexto que surgem os Sistemas de Informação (SI) de cariz policial, como estruturas basilares para as atividades de prevenção e combate ao crime e para um eficiente emprego e atuação dos meios policiais, através de processos de trabalho céleres, agilizados e consolidados.

Como refere José Braz, esta abordagem tem vindo a ser unanimemente reconhecida ao nível das Organizações Internacionais (OI) e das polícias de investigação, visando a



“*incontornável necessidade de dispor de sistemas de informação criminal, no âmbito dos quais se desenvolve um processo de tratamento em que a análise tem um papel fundamental. O investimento neste domínio, e muito particularmente na formação de analistas, tem natureza prioritária em muitas organizações policiais, sendo evidentes os esforços feitos no sentido de uniformizar procedimentos de modo a facilitar e potenciar a coordenação operacional e a cooperação internacional*” (Braz, 2009, p. 40).

Neste caminho é essencial estudar os SI policiais e criminais, sustentados em Tecnologias de Informação (TI), enquanto estruturas de suporte fundamentais na atividade das *informações*, edificados de acordo com as necessidades específicas de cada Instituição, viabilizando o processamento de uma multiplicidade de dados provenientes de diversas fontes e dinamizando o fluxo de informações, possibilitando a sua difusão atempada aos destinatários relevantes.

Quanto mais global e estruturado for um SI, encarado como o conjunto de meios humanos e técnicos, dados e procedimentos, devidamente entrosados e estruturados, mais eficiente será a análise de informações e, conseqüentemente, mais contribuirá para os objetivos últimos do trabalho das Instituições policiais, a prevenção e o combate ao crime e a segurança dos cidadãos e da sociedade em geral.

Justificação do Estudo

O tema objeto de engloba duas vertentes que, atualmente são indissociáveis, dada a complexidade do moderno ambiente social, o volume de dados administrativos, criminais e policiais, bem como de notícias e informações de fontes abertas, de grandeza tal que seriam impossíveis de registar, tratar e analisar sem ter por base sistemas de informação adequados, por forma a obter respostas mais eficientes.

Prendemos assim levar a cabo uma reflexão sobre o contributo das informações policiais (IP) (*intelligence*) para a eficácia da ação policial e para combate ao crime, com especial enfoque para o modo como FFSS encaram e operacionalizam a Análise Criminal (AC), nas vertentes estratégica, operacional e tática.

É inequívoca a importância das *informações* e do conhecimento, na atividade policial, sendo a análise uma fase essencial (e a função do analista por inerência) na sua produção, contribuindo para a atuação das FFSS na prevenção e combate à criminalidade, constituindo-se os SI num suporte essencial a todo o espólio informacional. Esta realidade aponta para a necessidade de refletir sobre a relação entre estas duas vertentes: SI e AC.



Sendo este o segundo ano em os que Oficiais da GNR têm oportunidade de frequentar o CEM C, parece-nos da maior relevância que seja dado destaque ao estudo dos assuntos do âmbito da Segurança Interna em geral, e das matérias policiais e criminais em particular, contribuindo para o conhecimento académico destas matérias e abrindo caminho a novas linhas de investigação e perspetivas doutrinárias para o IESM.

Objeto da Investigação e sua Delimitação

A temática do presente trabalho é a “Análise Criminal e Sistemas de Informação”, pretendendo-se relacionar estes dois conceitos e caracterizá-los numa perspetiva teórica, sublinhando a importância da AC para a produção das IP, e analisar a sua aplicação face aos SI das FFSS (Guarda Nacional Republicana (GNR), Polícia de Segurança Pública (PSP), Polícia Judiciária (PJ) e Serviço de Estrangeiros e Fronteiras (SEF)) no âmbito do Sistema de Segurança Interna em Portugal, enquadrando-os complementarmente nas consideradas “boas práticas internacionais”, nomeadamente no paradigma do policiamento orientado por informações – *Intelligence Led Policing* (ILP). Pretendemos ainda avaliar a adequabilidade dos SI implementados, a sua interoperabilidade e efetiva partilha de informação entre FFSS, à luz das necessidades da AC, como contributo para o processo de decisão policial aos diversos níveis estratégico, operacional e tático, nos âmbitos da prevenção e IC.

Definição dos Objetivos da Investigação

O objetivo geral desta investigação consiste em apresentar um estudo que contribua para a compreensão da importância das IP, em geral, e da AC, em particular, na prevenção e combate aos fenómenos criminais em Portugal, face aos SI policiais implementados nas FFSS, a sua interoperabilidade, e a coordenação e partilha de informação.

Esta investigação pretende explorar os seguintes objetivos específicos:

- Identificar o papel das *Informações* na atividade policial;
- Identificar o papel da AC nas IP, na atividade policial e na prevenção Investigação Criminal (IC), bem como na adoção de políticas de segurança;
- Caracterizar os SI utilizados em cada uma das FFSS, focando a interoperabilidade e a partilha de IP, na perspetiva da adequação ao trabalho dos analistas e à produção de *Informações*.
- Perspetivar a possibilidade de evolução da atividade da AC e dos SI.



Metodologia

No que respeita ao percurso metodológico, seguimos a abordagem adotada pelo IESM (Quivy & Campenhoudt, 1998), iniciando o trabalho por uma pesquisa bibliográfica e documental, recorrendo fundamentalmente a estudos e reflexões publicados, nacionais e internacionais, em variados suportes e aos diplomas legais adequados numa procura de diferentes perspetivas de análise, com o intuito de extrair as necessárias conclusões. Seguidamente com o objetivo de aprofundar a compreensão sobre as questões em análise e, certificar as respostas que fomos obtendo ao longo do percurso investigatório, com o intuito de alcançar resultados o mais integrais possível para as questões estabelecidas, optou-se pela realização de entrevistas semi-dirigidas a pessoas com vasta experiência profissional e conhecimentos técnicos e nas áreas da AC, das IP e da IC, procurando avaliar o modo como as temáticas em investigação são percecionadas por estes profissionais, quais as lacunas identificadas ao nível da análise e do funcionamento dos sistemas, procurando levantar ainda perspetivas futuras de evolução destas temáticas.

Este tipo de entrevistas, a mais utilizada em investigação social, “é semi-diretiva no sentido em que não é inteiramente aberta nem encaminhada [...] o investigador dispõe de uma série de perguntas, a propósito das quais é imperativo receber uma informação por parte do entrevistado” deixando que o mesmo fale abertamente pelas palavras que desejar sobre o assunto (Quivy & Campenhoudt, 1998, p. 192).

Na referenciação bibliográfica utilizámos o sistema autor-data, adotando-se o estilo Harvard-Anglia.

Completada a recolha dos dados necessários à investigação, realizámos a respetiva análise procurando extrair os dados essenciais para obter resposta às questões levantadas no início do percurso investigatório.

Para consolidar o modelo de análise, optámos pela forma indutiva aduzindo os conceitos operatórios isolados, no sentido do particular para o geral.

Estabelecido e delimitado o objetivo do trabalho, bem como as suas bases, motivações e a metodologia escolhida, é ainda essencial estabelecer e concretizar mais especificamente o que se pretendeu atingir com a sua realização, nomeadamente a pergunta de partida (PP) e as Questões Derivadas (QD) que nos orientaram ao longo da investigação.



Pergunta de Partida (PP):

No seguimento do exposto apresentamos como Questão Central (QC):

“Qual o contributo da análise criminal para a produção das informações policiais e criminais, face aos sistemas de informação implementados em Portugal?”

Para atingirmos os objetivos específicos, identificamos as seguintes QD:

- (QD1) – Serão as informações um importante pilar da atividade policial na atualidade?
- (QD2) – Qual o contributo da AC na atividade policial, de prevenção e IC, bem como para o desenvolvimento de políticas de segurança?
- (QD3) – Os SI das FFSS em Portugal respondem às necessidades da análise na produção de informações policiais e criminais?
- (QD4) – Como podem ser melhorados os SI das FFSS em Portugal para obter uma melhor resposta da AC no contributo para a prevenção e IC?

A cada QD alocámos uma Hipótese (H), que confirmaremos ou infirmaremos, sendo seguidamente descrito o seu articulado:

- H1: A atividade das FFSS carece de informações que suportem o processo de decisão policial e as atividades de prevenção e de IC.
- H2: A AC é um fator crítico para o planeamento da atividade policial e para a IC, bem como para a implementação de políticas públicas de segurança.
- H3: Os SI policiais existentes em Portugal são adequados enquanto instrumentos de suporte da AC e da produção de IP.
- H4: A interoperabilidade entre SI e uma efetiva partilha de Informações são indispensáveis para garantir o funcionamento eficiente da AC nas FFSS em Portugal.

Relativamente ao articulado do corpo do trabalho, estruturámos sequencialmente os diversos conteúdos nos termos seguintes:

No primeiro capítulo procurámos caracterizar o papel das *Informações* na segurança, começando por definir as *Informações* estratégicas e relacioná-las com as perspetivas policial e criminal. Definimos de seguida o papel das *informações* na atividade policial caracterizando-as, definindo o contributo que dão para o combate à criminalidade e para a prevenção através da orientação do policiamento e do trabalho desenvolvido pelas FFSS.



Caraterizámos ainda o Ciclo de Produção de Informações (CPI) (em apêndice 4) e o *Intelligence Led Policing* (ILP)¹.

No segundo capítulo focamos, com especial ênfase, a AC, nas vertentes estratégica e operacional e a função do analista criminal, numa perspetiva teórica, mas complementada com a visão da realidade das FFSS nacionais.

Já no terceiro capítulo enquadrámos conceptualmente os SI e as TI focando a sua importância na moderna gestão das organizações.

No quarto capítulo, focámos SI das FFSS em Portugal, avaliando suas potencialidades e limitações de resposta, bem como da interoperabilidade entre si, tendo em consideração que terão de ser compatibilizados para contribuir para a Plataforma para o Intercâmbio de Informação Criminal (PIIC)², atualmente em implementação.

Por fim, nas conclusões apresentamos a discussão dos resultados da investigação, respondendo às perguntas derivadas e arguindo a confirmação ou infirmação das hipóteses levantadas no modelo de análise e consolidamos a resposta à pergunta de partida.

¹ Tendo em conta o uso corrente do termos optamos por usar a sigla em inglês (ILP).

² Prevista nos termos na Lei n.º 73/2009, de 12 de Agosto, que estabelece as condições e os procedimentos a aplicar para assegurar a interoperabilidade entre sistemas de informação dos órgãos de polícia criminal (AR, 2009).



1. As *Informações* - Enquadramento Conceptual

A qualidade da ação policial depende muito da produção de informações: o conhecimento guia a inteligência policial serve o cidadão, protegendo-o de riscos maiores.

Pedro Clemente (2008, p. 25)

a. Das *Informações Estratégicas e de Segurança às Informações Policiais*

A missão nuclear das *informações* corresponde, segundo Sónia Reis, ao universo da segurança interna e externa e desenrola-se a montante da atividade de polícia (que no seu sentido mais comum consiste na manutenção da ordem pública) e da atividade de IC (que corresponde à tarefa de descobrir quem cometeu o crime), por não ser independente da existência de *notitia criminis* ou de necessidades concretas de manutenção de ordem pública (Reis & Silva, 2007, pp. 1252-1254).

A Lei-quadro do Sistema de Informações da Republica Portuguesa (SIRP) define, nos termos, no n.º2 do art.º 2.º, que “aos Serviços de Informações incumbe assegurar, no respeito da Constituição e da lei, a produção de *informações* necessárias à salvaguarda da independência nacional e à garantia da segurança interna”, estabelecendo claramente uma separação entre a atividade dos serviços, em cada um deles poderá apenas “desenvolver as atividades de pesquisa e tratamento das *informações* respeitantes às suas atribuições específicas”. Os Serviços que compõem o sistema são: o **Serviço de Informações Estratégicas de Defesa (SIED)**, organismo incumbido da produção de *informações* que contribuam para a salvaguarda da independência nacional, dos interesses nacionais e da segurança externa do Estado Português (art.º22.º), e o **Serviço de Informações de Segurança (SIS)**, organismo incumbido da produção de *informações* que contribuam para a salvaguarda da segurança interna e a prevenção da sabotagem, do terrorismo, da espionagem e a prática de atos que, pela sua natureza, possam alterar ou destruir o Estado de direito constitucionalmente estabelecido (art.º21) (AR, 2004). Estas atividades são atribuídas com caráter de exclusividade pelo art.º3, da Lei n.º 9/2007, de 19 de Fevereiro (AR, 2007).

Como nos refere Moleirinho, as *informações* de segurança têm como destinatários os órgãos de decisão política ou as chefias de topo das autoridades policiais, revestindo um carácter transversal que engloba fatores macroeconómicos, sociais, políticos e culturais, que abrangem dimensão regional, nacional e mesmo internacional, podendo assumir uma natureza meramente estratégica ou também operativa (Moleirinho, 2009, p. 81).



Quando incidem sobre questões de segurança, em sentido estrito, a atividade das *informações* visa prevenir a existência de circunstâncias propícias à prática de crimes ou à quebra da ordem e tranquilidade públicas, segundo Júlio Pereira (cit. por Reis & Silva, 2007, p. 1254) “as *informações* e a IC são duas realidades que convivem na atividade da segurança interna, que interagem na respetiva prossecução e que têm um ponto privilegiado de encontro no domínio da prevenção criminal”. A atividade das informações apresenta assim um carácter eminentemente preventivo, com o escopo de proporcionar ao poder político um conhecimento da realidade que possibilite a tomada de decisões fundamentadas em questões fundamentais para o interesse público e possibilitar a adoção de políticas públicas adequadas nesses domínios.

Constatamos assim que os Serviços de Informações em Portugal têm limitações legais que vedam as atividades eminentemente policiais (como efetuar buscas domiciliárias ou escutas telefónicas), tal não significa que, respeitados os limites legais, as atividades de polícia e IC não interajam, através de mecanismos de cooperação e coordenação (Reis & Silva, 2007, p. 1255), apesar da limitação que se verifica do “acesso a dados e informações na posse dos Serviços de Informações” requerer autorização do competente membro do Governo, “sendo proibida a sua utilização com finalidades diferentes da tutela da legalidade democrática ou da prevenção e repressão da criminalidade” (AR, 2004). Por outro lado a lei estabelece “uma clara distinção nos regimes de segredo de estado e segredo de justiça, que não admitem a sua consideração conjunta num sistema de vasos comunicantes” (Pereira, 2005, p. 156).

Concluimos assim que existe uma clara distinção entre *informações policiais e criminais*, por um lado, e *informações de segurança* por outro, que se perspetivam em planos diferentes. Enquanto as primeiras têm na génese da sua produção a prevenção criminal e de incidentes de ordem pública ou se inserem no âmbito de um concreto processo-crime; as últimas visam garantir a segurança nacional e produzir informação a nível estratégico, obstando também ações hostis de recolha de informação sobre as capacidades, objetos e vulnerabilidades nacionais (Moleirinho, 2009, p. 82).

Não obstante, como refere Rui Pereira, existirem fenómenos que interessam às *informações* e que nunca atingem o grau de precisão necessário à instauração de um procedimento criminal, ou, noutros casos as matérias podem interessar aos serviços de informações e estarem destituídas de relevância criminal (por exemplo, o investimento estrangeiro), situações há em que os fenómenos podem ser acompanhados em simultâneo por serviços de informações e órgãos de IC. Nesta última hipótese, são diferentes os ângulos de abordagem - por exemplo, os Serviços de Informações podem estar interessados num crime de



tráfico de droga, na medida em que ele revele uma fonte de financiamento do terrorismo, ao passo que os OPC, subordinados funcionalmente ao Ministério Público, procuram reunir indícios probatórios que habilitem a dedução de uma acusação no âmbito de um inquérito (Pereira, 2005, p. 159).

A importância das *Informações* enquanto garante de uma sociedade livre e democrática ficou patente nas palavras do General Pedro Cardoso, “*Quanto mais livre é uma sociedade, mais necessita de estruturas que a protejam. Uma dessas estruturas é sem dúvida um eficiente serviço de informações*” (Cardoso, 2004, p. 163).

b. As Informações Policiais

Na sociedade hodierna, o conhecimento constitui um fator estratégico na gestão operacional das Forças de Segurança, nas mais diversas áreas de atuação, e as informações guiam necessariamente a ação policial, favorecendo a previsão da ilicitude e o cumprimento da legalidade (Clemente, 2008, p. 11), considerando-se do maior interesse haver uma certa diversificação da atividade das *informações*, preconizando-se assim que as polícias beneficiem do estatuto de serviços de informações ao mais alto nível (Cardoso, 2004, p. 159).

As *IP* são aquelas destinadas à prossecução das missões policiais legalmente suportadas, num nível instrumental, mais estratégico-operativo, com o fim de suportar a atividade das estruturas operacionais (Torres, 2005, p. 593). Deveremos ter em conta que o conhecimento constitui um fator estratégico na gestão operacional das Forças de Segurança (FS) nas diversas atividades, como sejam, entre outras, a fiscalização seletiva de veículos, com o escopo de reduzir a sinistralidade rodoviária, o combate ao consumo de estupefacientes, ou o controlo de substâncias explosivas (Clemente, 2008, p. 11).

Se optarmos por caracterizar as *IP* com base no fim a que se destina a sua recolha e utilização, podemos assinalar a existência de “informações preventivas, criminais e de segurança *stricto sensu*”. “As primeiras têm na génese da sua produção a prevenção criminal e de incidentes de ordem pública; as segundas, por seu turno, inserem-se no âmbito de um concreto processo-crime; e as últimas visam garantir a segurança nacional e produzir informação a nível estratégico, obstando, entre o mais, também a ações hostis de recolha de informação sobre as capacidades, objetos e vulnerabilidades nacionais” (Moleirinho, 2009, p. 81). As FFSS podem, segundo Torres, “produzir qualquer tipo de informação, desde que revistam uma natureza instrumental e se insiram no âmbito das suas atribuições estatutárias, destinando-se portanto a consumo interno” (Torres, 2005, p. 593).

Pedro Clemente, por seu turno, em função da sua natureza, distingue entre *informações de ordem pública*, *informações criminais* e *contrainformações* (Clemente, 2008, p. 24) .

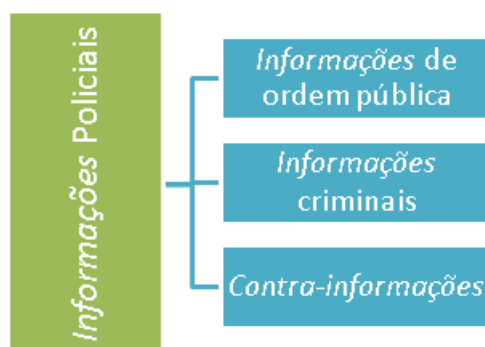


Fig.1 – Classificação das Informações Policiais

Fonte: Mário Fernando e Pedro Clemente (Clemente, 2008, p. 25)

Começaremos por explicitar as contrainformações, considerando tratar-se da atividade que visa impedir a realização de ações de recolha indevida de informação sigilosa e/ou classificada (confidencialidade, integridade e disponibilidade), no âmbito de toda a atividade policial e garantir o controlo de acessos apenas a pessoal credenciado e autorizado nas instalações policiais (Clemente, 2008, pp. 24-25). Esta atividade está intimamente ligada às “atividades de segurança, ativas e passivas, que incluem a implementação de medidas protetivas para impedir o acesso a instalações, equipamentos, sistemas de informação (segurança de sistemas), por parte de organizações, grupos ou indivíduos e negar o conhecimento da natureza, tipo, extensão e resultados das atividades” (GNR, 2012a, p. 8).

As *Informações* de ordem pública visam a prevenção de incidentes de ordem pública e acautelar a ocorrência de incividades, em particular a produção de delitos criminais, integrando o conhecimento resultante da atividade pré-processual em sede criminal (Clemente, 2008, p. 24).

Refira-se que a prevenção criminal é “uma função primordial e prioritária em qualquer Estado de direito democrático, cabendo em especial às FS envidar os necessários esforços para evitar a ocorrência de factos atentatórios das finalidades da atividade de segurança interna através da dissuasão, da vigilância, da fiscalização e controlo e da promoção de mecanismos de autoproteção entre os cidadãos” (Torres, 2005, p. 585).

Quanto às *Informações* criminais, podemos caracterizá-las como aquelas que se inserem na atividade reportada à IC. Segundo Torres, a IC pode ser definida (de modo lato) como o conjunto de diligências intelectualmente organizadas metodicamente sequenciadas, realizadas dentro dos limites previstos na legislação em vigor, oportunamente destinadas a apurar a existência dum crime, a descobrir os seus agentes e a esclarecer todas as circunstâncias julgadas relevantes para a graduação da sua culpabilidade e



responsabilidade, para aferição da sua personalidade e para a total delimitação das consequências efetiva ou potencialmente resultantes do ato ilícito (Torres, 2005, p. 589).

As informações constituem-se como elemento fundamental para a IC, constituindo a sua recolha um procedimento basilar a ter em conta pelos elementos policiais no local do crime, bem como pelos responsáveis pela inspeção judiciária e pela IC, pois nos termos da lei, “os órgãos de polícia criminal podem” recolher “informações relativas a um crime e, nomeadamente, à descoberta e à conservação de meios de prova que poderiam perder-se antes da intervenção da autoridade judiciária”.

Ferreira Antunes refere, a este propósito, que a informação criminal “funciona como um alicerce da estrutura que é a investigação” sendo “um elemento essencial do processo de investigação: sem informação, a panóplia de recursos tecnológicos, das tecnologias de informação e as capacidades e destrezas técnicas de investigação não tem qualquer utilidade e sentido, pelo que se verifica uma “dependência compulsiva da investigação relativamente à informação” (Antunes, 1999 cit. por Cruz, 2002, p. 23).

Considera o mesmo autor que as *Inteligência Policial* é o conjunto de ações que empregam técnicas especiais de investigação, visando a confirmar evidências, indícios e a obter conhecimentos sobre a atuação criminosa dissimulada e complexa, bem como a identificação de redes e organizações que atuem no crime, de forma a proporcionar um perfeito entendimento sobre a maneira de agir e operar, ramificações, tendências e alcance de condutas criminosas (Antunes, 1999 cit. por Cruz, 2002, p. 24).

Carter afirma que as *IP (Intelligence)* constituem o produto de um processo analítico que avalia a informação recolhida de diversas fontes, integra a informação relevante num produto consistente e produz uma conclusão ou estimativa sobre os fenómenos criminais através de uma perspetiva orientada para a resolução de problemas (e.g. recorrendo à análise). A *Intelligence* é um produto sinérgico que visa providenciar orientações significativas e confiáveis aos decisores policiais sobre criminalidade complexa, organizações criminais, extremistas e terroristas (Carter, 2004, p. 7).

Segundo o mesmo autor há dois propósitos essenciais para as informações numa força policial: a **prevenção** que inclui o ganho ou o desenvolvimento de informações ou conhecimento relacionado com as ameaças³ criminais ou terroristas, utilizando-a

³ A ameaça pode ser definida, no seu conceito tradicional, como “um qualquer acontecimento ou ação (em curso ou previsível), de variada natureza, proveniente de uma vontade consciente e inteligente e que impede a consecução de determinados objetivos; no fundo, o produto de uma capacidade por uma intenção” (Garcia, 2009, p. 5).

subsequentemente para a detenção dos suspeitos ou autores, proteger possíveis alvos e criar estratégias para eliminar ou reduzir a ameaça. Considerando tratar-se, neste caso de informações de nível tático.

O segundo propósito é o **planeamento e atribuição de recursos**, sendo que neste caso a função *intelligence* fornece informação aos decisores sobre a natureza das ameaças e as suas mutações, sobre as suas características, metodologias e idiossincrasias com vista ao desenvolvimento de estratégias de resposta e adequada aplicação dos recursos disponíveis com o objetivo de obter a adequada prevenção. Neste caso estaremos perante, informações de nível estratégico (Carter, 2004, p. 8).

Noutra perspetiva, segundo a classificação de Shulsky, podemos caraterizar as *informações*, numa perspetiva policial, como **produto**, como **conjunto de atividades**, ou **enquanto organização** (Shulsky, 2002, cit. por Lourenço, 2006, p. 1).

Como **produto** (conhecimento) resultante do processamento de notícias de carácter policial, traduzindo-se na denominada informação relevante para a atividade da polícia. Trata-se do *output* com valor acrescentado que permite compreender melhor algo relacionado com a atividade policial e contribuir para a tomada de decisão (Shulsky, 2002, cit. por Lourenço, 2006, p. 1).

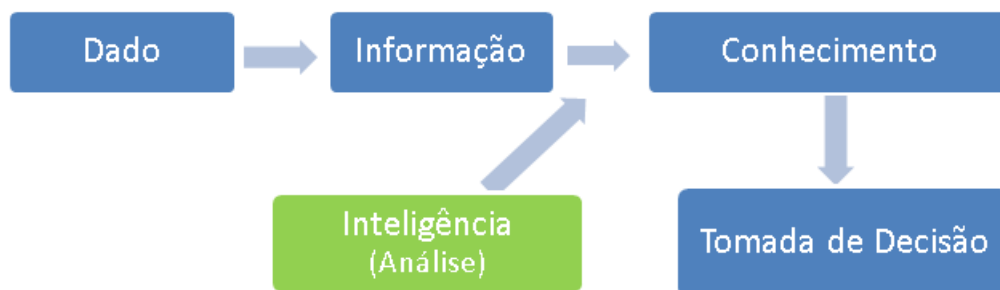


Fig.2 – Diagrama das Informações como produto.

Adaptado: (GNR, 2012b, p. 2)

Enquanto **conjunto de atividades**, as *informações* são desenvolvidas pelas polícias com o objetivo de obter o conhecimento, englobando a pesquisa (através de: HUMINT⁴; COMINT⁵, OSINT⁶, IMINT⁷, RADINT⁸ entre outras) e necessariamente a análise de

⁴ HUMINT (*Human Intelligence*)– é a Informação pesquisada/obtida através de fontes humanas (GNR, 2012b, p. 5).

⁵ COMINT (*Signals Intelligence*) - interceção dos sistemas de comunicações.

⁶ OSINT – (*Open Source Intelligence*) Informações que derivam fontes abertas (rádio, televisão, etc).

⁷ IMINT (*Imagery Intelligence*) informações obtidas através de imagens.



notícias, dados e factos que foram anteriormente recolhidos (através de técnicas específicas como é o caso da análise comparativa de casos ou da análise de grupos de autores) transformando os dados, factos e notícias em informação útil para a atividade policial potenciando a qualidade da decisão. Enquanto **organizações**, que atuam no desenvolvimento das atividades referidas, para produzir *informações* ou conhecimento útil aos seus desígnios (Shulsky, 2002, cit. por Lourenço, 2006, p. 2), por organizações nesta perspetiva podemos enquadrar os departamentos ou estruturas orgânicas que dentro das FS se dedicam a esta atividade específica.

Não podemos deixar de sublinhar que esta ordenação conceptual, não poderá configurar uma perspetiva estanque. Mas sim dinâmica em que as três vertentes estão interligadas pois as **organizações** (de informações) e suas **atividades** visam um fim último: o **produto** – as *informações* (*intelligence*) e o conhecimento.

As *IP* (produto) poderão ser classificadas em: **Informações Estratégicas, Operacionais e Táticas** (GNR, 2012b, p. 3). Esta classificação resulta do aumento da necessidade de especificidade da informação à medida que vamos descendo na estrutura hierárquica de uma instituição, uma vez que as tarefas a realizar na base incorporam problemas mais concretos, ao contrário do que acontece ao nível de topo, onde as preocupações são mais abrangentes, abarcando a generalidade das funções e as políticas institucionais (PJ, 2010, p. 2).

As Informações Estratégicas visam fornecer apoio aos decisores de topo (políticos / Comandantes) e, como tal, apresentam-se como um instrumento de gestão (Carter, 2004, p. 86). O estudo e análise dos fenómenos criminais servem de base à adoção de medidas relativas à condução das políticas de segurança, modelos ou programas de policiamento (programas de policiamento nacionais), ou medidas legislativas (por exemplo a política criminal) (GNR, 2012b, p. 3). Este tipo de informação tem objetivos de longo prazo, “tratando-se de uma especulação racional sobre futuros eventos criminais, a fim de preparar a melhor forma de os prevenir” (PJ, 2010, p. 7).

As **Informações Operacionais** são necessárias à adaptação das organizações policiais ao “ambiente” policial ou criminal, numa perspetiva de resposta organizacional (GNR, 2012b, p. 3). Têm por base dados gerais e estão relacionadas com a análise do fenómeno da criminalidade e das tendências de evolução no tempo e no espaço numa determinada área geográfica (nacional ou regional), numa ótica de orientação da atuação

⁸ RADINT (*Radar Intelligence*) - obtida de radares.



das unidades policiais e da gestão dos recursos das organizações para a prevenção e combate à criminalidade e manutenção da ordem pública (Lourenço, 2006, p. 4). Cita-se a título de exemplo o estudo da criminalidade (ex. criminalidade violenta e grave) em focando áreas geográficas, períodos horários, *modi operandi* e perfil de autores [...] com o objetivo de proporcionar orientações sobre a forma como as missões de policiamento, ou IC deverão ser efetuadas, definir tipologias criminais prioritárias para combater (ex. roubos, furto de caixas multibanco ou furto de metais não preciosos), dotar as unidades locais com os meios (humanos e materiais adequados) ou definir operações de âmbito nacional (ex. combate à criminalidade rodoviária).

As **Informações Táticas** têm como objetivo de apoiar as unidades de nível tático ao nível das pequenas unidades (Destacamentos Postos, Esquadras, Unidades de IC e são necessárias ao planeamento e condução de operações de segurança, ordem pública ou condução da IC (GNR, 2012b, p. 3). Fundamenta-se em dados concretos, destinam-se à compreensão de um assunto em particular e têm objetivos de curto prazo. Visam a definição de ações policiais concretas, nomeadamente, buscas, rusgas, vigilância, capturas de suspeitos ou operações de fiscalização, entre outras (Lourenço, 2006, p. 4). As informações táticas são também utilizadas para apoiar o processo de decisão de um comandante que enfrenta uma situação (ou incidente) tático policial grave⁹ (Carter, 2004, p. 86).

⁹ Definido no Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança (PCCCOFSS). Por exemplo: ataques a órgão de soberania (SSI, 2008).



c. O Policiamento Guiado por Informações (*Intelligence Led Policing*)

Pela Europa e América do Norte tem-se verificado uma tendência por parte dos serviços policiais para abordagens proativas orientadas para os problemas. Em alguns sistemas tem vindo a ser desenvolvida a denominada *Intelligence Led Policing (ILP)*.

O modelo de policiamento foi emergindo, no Reino Unido¹⁰, de uma postura reativa das Forças de Segurança, primeiro como uma atividade periférica efetuada apenas em unidades especializadas para se tornar num modelo abrangente das policiais em geral, não apenas naquele país e nos EUA, mas em muitos outros, embora com variantes e níveis de desenvolvimento diversificados. Para tal concorreram diversos fatores como a noção de que os modelos tradicionais não respondiam às necessidades emergentes, com falhas evidentes no sistema criminal, respondidas inicialmente com um aumento de efetivos policiais, sem os correspondentes ganhos de eficiência (Flood, 2004, cit por Ratcliffe, 2011, p. 266).

Esta situação gerou pressões para um aumento para a melhoria da ação policial pelo poder político (seguindo a tendência do “*new public management*”), que colocou as chefias policiais perante a necessidade de alterações na administração, em particular na análise e gestão do risco, dado o escrutínio a que estavam sujeitas, conduziu a uma necessidade de incrementar a atividade das informações no suporte à decisão (Ratcliffe, 2011, p. 265).

Com o fim da guerra fria e a abertura das fronteiras no espaço europeu, que conduziram a alterações de fundo na cena internacional, o crime organizado teve condições

¹⁰ Cita-se o *National Intelligence Model* Britânico (NIM) como o modelo de referência do ILP. O NIM é um produto do *National Criminal Intelligence Service* (NCIS) do Reino Unido (RU), promovido pela *Association of Chiefs of Police*. Todo o desenho e teste do modelo foram completados por polícias, analistas e especialistas de informações das diversas Forças e Serviços de Segurança daquele país. O sistema representa a compilação do conhecimento e das melhores práticas no policiamento guiado por informações e atuação policial. O modelo visa prover o enquadramento para orientação de uma estratégia efetiva, não apenas no que concerne ao crime e aos criminosos, mas incluindo todo o espectro de atividades das organizações policiais, desde a o crime organizado à segurança rodoviária.

O NIM foi desenhado com o objetivo de profissionalizar a disciplina (área do conhecimento) das informações nas Forças de Segurança através da implementação de uma doutrina comum de informações, estabelecendo a forma como as lideranças deverão atuar e como a informação deverá ser pesquisada, registada, analisada e difundida e partilhada, contribuindo quer para o processo de decisão (a nível estratégico) quer para a operacionalização dos programas de policiamento e orientação dos meios táticos no combate ao crime.



para florescer, potenciado pela globalização, a criação das transações financeiras eletrónicas e a disseminação da internet. Estávamos no fim de uma era em que os departamentos policiais podiam trabalhar isolados a nível nacional e internacional, gerando a necessidade de serem estabelecidas posturas mais colaborativas entre os departamentos policiais, associadas a reorganizações internas (promovendo estruturas específicas de trabalho dedicadas ao crime transnacional¹¹ (e.g. grupos específicos – máfias russas, organizações asiáticas...)) e às ligações com atores internos, bem como à criação de novos modelos de policiamento, com novas linhas conceptuais de atuação que servissem de orientação à sua atuação (Ratcliffe, 2011, p. 266).

Por outro lado verificaram-se avanços significativos nas tecnologias de informação, que foram sendo adotadas pelas FS desde meados da década de 1970. Originalmente o seu uso era eminentemente para coligir estatísticas para informar os governos e para a gestão administrativa (Ericson, 1997, cit por Ratcliffe, 2011, p. 266), contudo foi progressivamente percecionada a vantagem do uso destes sistemas na gestão dos grandes volumes de informação policial. É assim que começam a surgir os analistas criminais nos departamentos policiais, defendendo que as informações deverão ser usadas para dar suporte à decisão tática dos comandantes de escalões intermédios e para criar uma perspetiva estratégica aos decisores de topo (Ratcliffe, 2011, p. 266).

Segundo Ratcliffe o *ILP* é um “modelo de negócio” é uma filosofia de gestão em que a AC se constitui como um pivô para um objetivo, ao nível do enquadramento do processo de decisão, no sentido de contribuir para a prevenção, redução e neutralização das atividades criminais e das alterações da ordem pública, através da gestão estratégica e da implementação de estratégias de implementação eficazes, visando os infratores que atuam de modo reiterado e com maior gravidade (Ratcliffe, 2011, p. 269).

O modelo requer uma grande integração das Informações criminais e da AC melhorando a gestão do risco em suporte do policiamento proactivo. Esta abordagem requer dos líderes policiais uma aprendizagem e um novo quadro mental para adotar uma nova forma de pensar sobre as informações e o risco, promovendo novas abordagens organizacionais, em especial no que concerne às secções de informações e aos analistas, com os quais devem estar em contacto frequente (Ratcliffe, 2007, p. 2).

¹¹ E.g. O *Department of Homeland Security* - nos EUA, o *Serious and Organised Crime Agency* (SOCA) - no RU, o *Criminal Intelligence Service Canada* (CISC), o *Australian Crime Commission* (ACC) e a *Australian Federal Police* (AFP).

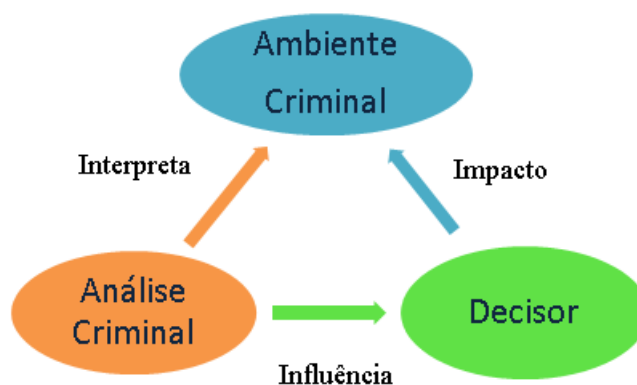


Fig.4 – *Intelligence Led Policing* – Modelo dos 3I.
Fonte: Ratcliffe 2003

No modelo apresentado, 3 I (Interpretação, Influência, Impacto) a capacidade analítica da polícia interpreta o ambiente criminal com o objetivo de determinar quem são os intervenientes principais e quais são as ameaças emergentes mais significativas que estão a emergir. Esta representação que “colide” com o ciclo de produção de informações, é mais realista, segundo o autor, pois aqui o analista procura analisar o ambiente, tendo um papel de motor do sistema, procurando a informação em contato com os agentes do terreno, em vez de de enviar “*information requests*” e esperar que a informação lhe seja remetida. Higgins (2004) considera que o ciclo de produção clássico não funciona porque a estrutura e cultura burocrática das Forças de Segurança “joga contra” a comunicação efetiva por “*intelligence requirements*”, pois grande volumes de informação não são passadas a escrito, mas permanecem apenas nas mentes dos agentes, ficando indisponíveis para partilha (Higgins 2004, cit. por Ratcliffe, 2011, p. 266). Perante este quadro, com o qual, fruto da experiência que detemos na matéria, concordamos, o analista neste modelo deverá contactar e “debrifar” os elementos operativos.

A influência aos decisores constitui-se numa parte essencial do modelo. Ao analista cabe efetuar recomendações baseadas na análise que efetuou, já a capacidade de decidir sobre a adoção das recomendações e direcionar a ação será competência do decisor, que tem aqui um papel fundamental. Quando se verifica uma resistência por parte das lideranças, por falta de formação ou sensibilidade o processo não terá o sucesso pretendido. É essencial que aspetos sensíveis sejam resolvidos pela liderança, como sejam questões tecnológicas, aspetos legais e de confidencialidade (para maximizar a partilha de informações) estabelecimento de contactos externos, e a formação sobre os modelos de policiamento relacionados, como o policiamento comunitário ou o policiamento orientado para o problema, e ainda assegurar um aspeto essencial, que os dados e a informação



existente é suficientemente completa, credível e está disponível para os analistas trabalharem e produzirem “artigos” de qualidade (Ratcliffe, 2007, p. 3).

Os desafios deste modelo requerem esforços de implementação no sentido da modernização policial, sendo fundamental que os dirigentes tomem as medidas necessárias para ultrapassar as barreiras culturais e organizacionais para tornar o ILP efetivamente uma realidade (Ratcliffe, 2011).

De acordo com Bratton, este tipo de policiamento pode ser definido como o combate ao crime orientado pela pesquisa e análise de informações, tendo este modelo, para os autores, o potencial de se constituir na mais importante inovação na ação policial no século XXI, uma vez que integra as estratégias já existentes e a tecnologia numa abordagem planeada para a adequada e eficiente gestão dos recursos disponíveis. Contudo, se não existir uma estratégia nacional ou os mecanismos necessários à sua implementação (e.g. liderança, formação e tecnologia), não passará de uma “intenção na prateleira” (Bratton & Kelling, 2006, pp. 6-8).

Para sublinhar a importância que este modelo de policiamento tem a nível Europeu, atentemos às palavras de Rob Wainwright, diretor da EUROPOL¹² que refere que “A estratégia de segurança interna da União Europeia prevê um papel fulcral para o Serviço Europeu de Polícia [...] para combater a criminalidade organizada e o terrorismo. No cerne da estratégia está um modelo acordado de segurança europeia assente num *ILP*. Isso contribuirá para definir prioridades comuns da União Europeia e compreender melhor as ameaças à segurança interna da União. O *ILP* tem sido um conceito-chave que subjaz a todas as atividades estratégicas de avaliação da Europol (EUROPOL, 2011, p. 5).

¹² A EUROPOL é a agência da União Europeia (EU) responsável pela aplicação da lei, tendo por missão apoiar os Estados-Membros na prevenção e no combate a todas as formas de criminalidade e terrorismo internacionais graves. O seu papel é contribuir para a consecução de uma Europa mais segura em benefício de todos os cidadãos da União, apoiando as autoridades comunitárias responsáveis pela aplicação da lei através do intercâmbio e da análise de dados em matéria de criminalidade (EUROPOL, 2011, p. 7) .



2. Análise Criminal

“As maiores falhas no âmbito das informações constituem falhas de análise, não de recolha ou pesquisa”¹³ (Heuer, 1999)

As atividades das FFSS têm sido, ao longo do tempo, guiadas por formas mais ou menos improvisadas de análise, uma vez que os elementos policiais recolhem informação da qual extraem conclusões sobre a natureza do crime, bem como sobre os seus autores e motivações. Contudo, constata-se que num sistema baseado numa abordagem puramente reativa ao crime, as informações desempenhavam um papel menor, sendo raramente usadas de modo coordenado e proactivo, mas apenas como simples ferramenta de suporte às investigações aplicada caso a caso (Ratcliffe, 2011, p. 263).

Após a década de 90, verificou-se uma forte evolução técnica e dos métodos, incrementando a importância da AC no desenvolvimento de estratégias efetivas de resposta aos problemas enfrentados pelas FS, de modo criativo e com proactividade, substituindo progressivamente uma postura reativa sobre eventos já ocorridos. Desde então verificou-se uma evolução vertiginosa neste campo. Atualmente, mesmo nos locais mais remotos as polícias podem ter já acesso a ferramentas informáticas e comunicações necessárias para se atingir um elevado nível na capacidade de análise do crime (IACP, 2001, p. 2).

Os agentes com funções policiais, no decurso das suas atividades diárias, recolhem enormes quantidades de dados, notícias e de informação, que se devidamente analisada pode ajudar diretamente nos esforços de prevenção e combate à criminalidade, inclusivamente ao nível das ações de IC, permitindo estabelecer ligações entre eventos, fatos, pessoas ou materiais (Osborn, 2006, p. 1), contudo, em muitas situações a informação é confinada aos indivíduos (investigadores) ou dentro de unidades especializadas, e até por analistas não sendo partilhada em prol da ação policial (Ratcliffe, 2007, p. 1), sendo certo que as *informações* são a base para a condução das operações e possibilitar o uso eficiente dos recursos policiais, através da criação de estratégias de atuação, bem como para a condução com sucesso das ações de IC, como foi enfatizado em

¹³ Esta questão ganhou particular relevância quando, na sequência da investigação aos atentados de 11 de Setembro nos Estados Unidos da América (EUA), se constatou que existia informação disponível nas várias polícias que, se devidamente partilhada e analisada, poderia ter levado à descoberta e prevenção dos atentados (Osborn, 2006, p. 3)



obras como “*Intelligence Led Policing*” e “*Guidelines for Starting an Analytic Unit*” (IACP, 2001, p. 2).

Contudo, quem está disponível para analisar toda a informação? Até que ponto é que essa informação é efetivamente partilhada e disponibilizada a quem dela necessita? Serão os analistas em número suficiente e estarão adequadamente preparados para as funções que desempenham?

a. Definição e caracterização

“O futuro da ação policial está na capacidade de rentabilizar a análise criminal e a tecnologia, com ética e bom senso, em suporte das políticas criminais” Marilyn Peterson (cit. por IACP, 2001, p. 3)

Mas em que consiste então a AC?

As definições são múltiplas¹⁴, variando entre países, FS, pelas dimensões e/ou grau de especialização das forças policiais, ou a geografia, sendo passível contudo encontrar uma matriz comum às diversas abordagens, o estudo do crime com o objetivo de melhorar a ação policial. Assim consideramos que a AC “consiste no estudo sistemático dos fenómenos criminais e de situações de desordem, tendo por base fatores sócio demográficos, espaciais e cronológicos” (PJ, 2010, p. 6), direcionado para fornecer informação pertinentes e atempadas relativamente a padrões criminais e correlação de tendências, para apoiar as forças policiais na avaliação, prevenção e combate aos eventos criminais e desordens públicas (Boba, 2008 cit. por Osborn, 2006, p. 13).

A análise serve de base à decisão estratégica, mas também orienta a aplicação dos recursos ao nível tático, podendo ainda ter um papel na identificação de boas práticas e lições aprendidas, através do estudo da atividade policial em ambos os níveis (NPIA, 2008, p. 10).

Constatamos assim que os campos em que atividade da AC pode ser usada são vastos e incluem o apoio para: a resolução de processos-crime; a detenção de criminosos; o desenvolvimento de estratégias e táticas para a prevenção do crime; o estabelecimento de melhorias na segurança da atuação policial; a otimização de operações; a priorização de

¹⁴ Ratcliffe, a título de exemplo, distingue entre análise de *informações (intelligence analysis)* e AC (*crime analysis*), considerando que a primeira enquadra o desenvolvimento de produtos críticos e em suporte do processo de decisão policial, centrado nas atividades relativas ao crime organizado. Já a AC envolve o uso de diversos tipos de informação geográfica e sociodemográfica, combinada com técnicas espaciais para analisar, prevenir e resolver o crime e as alterações da ordem (Ratcliffe, 2007, p. V).



patrulhas e investigações; as melhorias na alocação de recursos, inclusive a nível administrativo (orçamental e planeamento organizacional) (Dantas & Souza, 2004); o planeamento de necessidades futuras; o estabelecimento de normas de atuação ou o apoio na educação dos cidadãos. O analista pode constituir-se assim num elemento essencial em suporte da missão geral de uma organização policial (Christopher, 2008, p. 7).

b. Análise Estratégica e Análise Operacional

A categorização reconhecida em termos europeus subdivide a análise em duas grandes categorias: a **Análise Estratégica** e a **Análise Operacional** (noutras correntes designada como análise tática) (PJ, 2010, p. 7).

À **Análise Estratégica** cumpre identificar as problemáticas de longo prazo numa área, bem como as projeções relativas à evolução das diversas tipologias criminais, permitindo às FS o estabelecimento de prioridades, a definição do emprego dos recursos, suportar o planeamento e fornecer informação às chefias de topo e ao nível dos decisores políticos (IACP, 2001, p. 3).

A análise estratégica, enquanto instrumento de apoio policial, contribui em Portugal necessária e significativamente para a tomada de decisão estratégica e para a implementação de políticas de prevenção criminal. A cabal compreensão dos fenómenos criminais, mediante as mais diversas metodologias de AC, permitirão orientar o esforço das Subunidades policiais na aplicação de determinadas medidas preventivas (podem contar com a colaboração de entidades externas na concretização de campanhas) (Fernandes, 2013) e de cariz operacional (ações direcionadas para locais específicos e/ou indivíduos/grupos suspeitos), pela identificação de MO e indicadores (indícios técnicos), que no conjunto permitirão o direcionamento do patrulhamento e o estabelecimento de prioridades (desde a formação inicial até à criação de programas especiais), estabelecer o perfil das vítimas (permitindo a adoção/recomendação de medidas passivas e ativas direcionadas) e também de identificar *clusters* (ou zonas de maior incidência de atividade criminal), possibilitando assim, também, a mais racional distribuição de meios (Grenho, 2013).

Cita-se a título de exemplo a emergência de “novos fenómenos” criminais, como o furto de caixas multibanco, o furto de metais não preciosos, ou os fenómenos de “*carjacking*”, cujo impacto gerou uma quase “obrigatoriedade institucional” de monitorar as ocorrências que lhe são características e perceber as dinâmicas dos indivíduos/grupos que estão associados, a comunicação com as diferentes Instituições policiais (nacionais e internacionais) e não policiais (SIBS e entidades bancárias, associações de empresários),



com vista à congregação de esforços que funcionassem como alerta e, também, como travão do crescente número de casos praticados (Fernandes, 2013). Estas medidas, têm contudo, uma mais vertente reativa do que a desejada proatividade, no âmbito da tomada de decisão estratégica (Borges, 2013), dado que mesmo quando geram alterações são geralmente uma consequência da evolução dos fenómenos e não os antecipam, como seria expectável.

Na GNR há uma dimensão da AC desenvolvida, que é muito importante para a prossecução e pra a eficiência da prevenção criminal, contribuindo para a qualificação dos contributos da Guarda para as decisões sobre as políticas neste domínio da segurança interna e para a adequada implementação dessas políticas (Pereira, 2013). Verifica-se contudo que o SIIOP apresenta fragilidades estruturais (e estruturantes) pelo fato de ter uma cobertura reduzida no território nacional. Este problema específico não afeta a do mesmo modo a PJ e a PSP, cujos sistemas cobrem toda a área de responsabilidade.

Relativamente à PJ é efetuado um acompanhamento de alguns fenómenos criminais que são considerados mais sensíveis (e.g. criminalidade violenta, criminalidade informática, droga ou crimes sexuais), no entanto, Paulo Gomes considera não poder aferir se a documentação produzida influencia o patamar estratégico (Gomes, 2013).

A **Análise Operacional** visa identificar as problemáticas de curto prazo numa determinada área, com o objetivo de prevenir a situação de se deteriorar, prestando apoio a operações correntes e ao planeamento, na reafectação de recursos e esforços, de acordo com as alterações das necessidades decorrentes da evolução das problemáticas. Além disso, a análise tática deverá providenciar uma imagem detalhada de potenciais suspeitos e das suas ligações para ações subsequentes, apoiando assim a gestão operacional a selecionar alvos, guiar investigações, adequar planos e manter a supervisão e controlo (IACP, 2001, p. 3).

Em Portugal, de um modo geral a AC é tida como uma vertente essencial ao nível da IC, em geral em todas as FFSS (Borges, 2013). Na GNR foi considerada determinante na definição das linhas orientadoras das investigações criminais resultando uma melhorada eficiência no decurso da atividade investigatória e eficácia melhorada nos resultados finais obtidos, citando-se o estabelecimento de Ficheiros de análise (*Analyst Working Files - AWF*) sobre temáticas específicas¹⁵ (Rocha, 2013).

¹⁵ Cita-se a título de exemplo os crimes de furto de metais não precisos ou a criminalidade itinerante.



Ao nível da PJ, existem níveis diferentes de avaliação da informação que contribuem para a eficácia da investigação. Uma avaliação de antecedentes é feita com os elementos iniciais da ocorrência, podendo ser feito um acompanhamento num processo de análise operacional em paralelo à investigação, com especial enfoque em análises de caso e de grupos de autores, dependendo da tipologia do crime (Gomes, 2013), sendo que no SEF a sua utilização primordial é feita ao nível das “investigações mais complexas e de cariz transnacional” (Marques, 2013).

O Departamento de IC da PSP monitoriza diariamente as ocorrências criminais que poderão estar associadas a fenómenos criminais com impacto transregional e transnacional. O manancial de informação difundido é canalizado para o dispositivo, que comporta uma rede nacional de analistas, com o objetivo de contribuir para o desenvolvimento das investigações em curso e para a adoção de medidas preventivas de carácter operacional, contribuindo com informação útil no momento certo (Vieira, 2013). É sublinhado a orientação para que os Comandos locais contribuam com notícias/informações relativas a eventuais fenómenos criminais, mediante indicações expressas em sede de Relatórios de Informações Criminais produzidos, sublinhando Urge orientar o esforço na recolha e processamento da informação proveniente das FFSS e, inclusive, das autoridades policiais estrangeiras (em especial aos adstritas aos Estados-membros da União Europeia) (Fernandes, 2013) (Grenho, 2013).

Santos, sublinha que a AC poderia ser mais potenciada, porque os “processos de negócio”, ou metodologias de trabalho, no âmbito da AC e IC deveriam ser assistidos por sistemas de informação acreditados, bem dimensionados às “necessidades de informação” e “contextos de utilização” dos diversos tipos de intervenientes, por forma que a recolha de dados e consequente análise permitisse chegar ao “conhecimento policial” sobre os fenómenos criminais que diretamente ou indiretamente lhes estão interligados (Santos, 2013), identifica assim uma lacuna nos SI que trataremos adiante neste trabalho.

c. A função do Analista Criminal

O analista criminal é, como nos refere Carter, um profissional que perante uma variedade de fatos, documentação circunstancial, provas, inquirições e outros materiais relacionados com um crime, os enquadra segundo um raciocínio lógico com o propósito de resolver um processo-crime, explicar um fenómeno criminal, ou descrever as tendências criminais (Carter, 2004, p. 110).



A complexidade das matérias inerentes à realização de AC exige um elevado nível de especialização ao analista para que esteja apto a exercer as suas funções de forma eficaz. O ideal para o analista é poder realizar o seu trabalho em dedicação exclusiva, sem ter que exercer outras funções. É necessário que a utilização dos métodos seja realizada metodicamente e no momento oportuno (PJ, 2010, p. 6).

O desenvolvimento do papel dos analistas de atividade criminal poderá constituir-se num multiplicador de capacidade na melhoria da segurança pública, reduzindo os índices de criminalidade e incrementando a segurança da sociedade (Osborn, 2006).

Nesta perspetiva, o envolvimento das lideranças é essencial para uma adequada implementação das capacidades de análise nas FS, através da demonstração de que há ganhos relevantes de custo benefício para as Instituições, pelo incremento da produtividade na resolução dos problemas reais do dia-a-dia, não apenas numa perspetiva reativa mas, essencialmente, através da antecipação das atividades criminais e dos fatos que afetam o cumprimento da missão policial. A questão que se coloca é: Como é que se consciencializam as chefias policiais para o potencial das informações? (IACP, 2001, p. 6).

Como é que se pode avançar num processo de qualificação ao nível das IP e criminais, se não existirem analistas, se forem em número insuficiente para as necessidades, ou se, apesar de assim designados, não tiverem formação que os qualifique e certifique (não passando de pesquisadores ou “simples administrativos” a inserir informação), e embora não por sua responsabilidade, sejam incapazes de produzir verdadeiros produtos analíticos, havendo ainda outros casos em que, por incompreensão das chefias, estes recursos, já de si escassos, são usados como simples amanuenses ou empregues em atividades administrativas correntes (IACP, 2001, p. 6).

Procurando espelhar a situação nacional relativamente aos analistas das FFSS, podemos afirmar, que o número de analistas, regra geral é insuficiente para as necessidades, este foi o quadro apontado, com as ressalvas de que muitas vezes a se verifica uma inadequação do trabalho do analista às suas funções específicas, e a sua rentabilização não é efetuada do mesmo modo ao longo do Dispositivo das diversas FFSS.

A PSP dispõe de analistas criminais em todo o seu dispositivo, considerando que “os meios humanos nunca serão os suficientes face às constantes mudanças e necessidades funcionais, pelo que se exige uma rentabilização de recursos” (Vieira, 2013). Todos os elementos têm formação específica, nomeadamente o “Curso de Análise de Informações Criminais” (Fernandes, 2013).



Na GNR, verifica-se que os analistas previstos em quadro orgânico (IC) são os adequados, contudo, fruto dos constrangimentos orçamentais, não tem sido formado o número necessário de elementos. Além disso muitos dos elementos que desempenham essa função não tem habilitação técnica, acrescendo que as ferramentas específicas (e.g. licenças de i2) são praticamente inexistentes (Rocha, 2013; Pereira, 2013). Quanto à Direção de Informações os meios em causa são extremamente insuficientes, prejudicando seriamente e mesmo comprometendo, em alguns casos, os desejados resultados operacionais que ficam muito aquém dos possíveis e desejáveis (Borges, 2013).

Na PJ verifica-se uma “real falta de recursos humanos e materiais” para funções de AC (Gomes, 2013), verificando-se que a Instituição possui um curso específico de AC, para habilitar os seus analistas.

O SEF possui elementos com competências para a função, bem como ferramentas (tecnológicas/informáticas) adequadas (Marques, 2013).

Pode assim concluir-se que, em termos gerais os meios necessários para uma adequada ação dos analistas criminais, em todo o Território Nacional não são de todo suficientes, ainda mais tendo em consideração a quantidade de fenómenos a sua diversidade e a própria mutação carecem de contínuo acompanhamento, resultando numa análise puramente reativa aos fenómenos e não numa perspetiva mais preventiva (Branco, 2013).

A criação de uma doutrina única de informações, à semelhança do que se verifica noutros países (e.g, NIM Britânico, ou até na EUROPOL, a nível europeu), foi considerado um passo fundamental por todos os entrevistados, com duas exceções, alegando questões de cultura Institucional e diferenças de competências, os dois exemplos citados são a prova de que qualquer destes aspetos não será minimamente impeditivo, pelo contrário, exigirá que esse passo seja dado.

O SG SSI dispõe já de competências de coordenação da ação e das ações conjuntas de formação, aperfeiçoamento e treino das FSS (artº 16º da LSI). Nos termos da alínea c) do nº3 do artº 16 compete-lhe ainda estabelecer com o Secretário-Geral do Sistema de Informações da República Portuguesa mecanismos adequados de cooperação institucional de modo a garantir a partilha de informações. Neste âmbito este seria um dos possíveis fora de discussão do tema para a criação de doutrina única (Grenho, 2013).



3. Sistemas de Informação - Enquadramento concetual

a. Os Sistemas de Informação

Os Sistemas de Informação visam a satisfação das necessidades de informação dos processos de negócio da organização, através de um conjunto de componentes interrelacionados que reúnem ou procuram, processam, armazenam e distribuem informação, destinada a suportar o processo de tomada de decisão e o controlo de uma organização (Laudon e Laudon, 2006, cit. por Martins, 2008, p. 27), constituindo uma ferramenta imprescindível ao processo de tomada de decisão aos vários níveis de gestão.

Com o advento do computador as técnicas de registo e manipulação de dados sofreram profundas alterações, em particular a partir dos anos 1990, quando a «procura» nos SI passou a ser impulsionada pela necessidade de obtenção de vantagens competitivas ou, pelo menos, de evitar desvantagens competitivas nas organizações. Com a difusão generalizada da Internet, no início do séc. XXI, a disseminação dos sistemas pelas organizações públicas e privadas passou a ser uma prioridade na agenda dos decisores, devido à diminuição dos custos de relacionamento e, em particular devido à mobilidade das comunicações que criaram novas oportunidades de melhoria de produtividade e eficiência em todas as organizações (Pereira, 2005, p. 14).

Para possibilitar uma melhor perceção da temática em apreço, começaremos por explicitar os conceitos chave.

“**Dados**” são fatos ou eventos, imagens ou sons que podem ser pertinentes ou úteis para o desempenho de uma determinada tarefa, mas que por si só não conduzem à compreensão desse fato ou situação (Rascão, 2004, p. 22). Podem resultar da interação de uma organização com o meio envolvente, têm formatos diversificados e muitos representam pouco valor para as tarefas essenciais da organização (Pereira, 2005, p. 15).

Numa organização, os dados passam a ser considerados “**informação**” quando, processados e agrupados num subconjunto, são úteis e acrescentam valor à tomada de decisão (Pereira, 2005, p. 15), e estão relacionados ou associados a algo que, fazendo sentido, ajuda a compreender determinados fatos ou um evento. Esta passagem dos dados a informação é efetuada através de processos de filtro, sumarização e formatação (Rascão, 2004, p. 22).

Quando as pessoas submetem a informação a processos de interpretação e atuam e decidem com base nesta e no seu conhecimento acumulado acerca de uma determinada situação, os seus resultados alimentam o processo de acumulação de conhecimentos. Esta acumulação habilita as pessoas para transformar dados em informação. O conhecimento



resulta assim da combinação de instinto, ideias, regras e procedimentos que guiam as ações e decisões (Rascão, 2004, p. 22).

No âmbito da teoria das informações, em geral, e das IP, em particular podemos referir, de modo sucinto, que a informação traduz o conjunto de dados contextualizados no espaço, no tempo e no cenário de ação, enquanto, as *informações* exprimem o sistema de recolha, de análise e de processamento de informação, para obter um conhecimento acrescido sobre certa situação específica - a inteligência é a informação relacionada, sistematizada e contextualizada (Clemente, 2006, p. 95).

Segundo Lucas (Lucas, 1987 cit. por Rascão, 2004, pág.26), “um sistema de informação é um conjunto organizado de procedimentos que, quando executados, produzem informação para apoio à tomada de decisão e ao controlo das organizações”. Constatamos que todo o processo de decisão está baseado no conceito de informação que está suportada nos SI das organizações.

Um sistema de informação representa todas as componentes dinâmicas da organização que incluem, entre outros, o *hardware*, o *software*, as regras e metodologias de desenvolvimento, as pessoas e a estrutura da organização que permitem recolha e a agregação de dados, a sua análise e apresentação de forma a tornar mais eficientes os processos administrativos e mais eficaz o processo de decisão (Pereira, 2005, p. 18).

b. As Tecnologias de Informação (TI)

Definidos Sistemas de Informação (SI), torna-se essencial definir Tecnologias de Informação (TI), tendo em vista o pressuposto de que a distinção entre elas é fundamental na adequada gestão organizacional, visto que a informação ajuda os gestores a tomar as decisões, seja qual for a tecnologia de suporte. Mas os gestores não poderão esquecer-se de que, numa organização do séc. XXI, será muito difícil obter vantagens competitivas sem o suporte das TI adequadas (Rascão, 2004, p. 27).

Assim, TI podem ser definidas como o conjunto de conhecimentos, de meios materiais (infraestruturas) e de *know-how*, necessários à produção, comercialização e ou utilização de bens e serviços relacionados com o armazenamento temporário ou permanente da informação, bem como o processamento e a comunicação da mesma.

Assim, se um SI é composto por: tecnologia do processo¹⁶, tecnologia do produto¹⁷, o produto¹⁸, a organização¹⁹ e as pessoas²⁰, as TI apenas compreendem o computador e o

¹⁶ O computador (equipamento físico) e infraestruturas de suporte (ex. estruturas de rede).



software que permitem o armazenamento físico da informação, processá-la e disponibilizá-la sempre que necessário. A TI é o uso dos recursos computacionais para o desenvolvimento de SI (Furtado, 2002, p. 24)

A escolha dos diversos tipos de *hardware*, das formas de comunicação de dados entre os diversos computadores, das linguagens e produtos de desenvolvimento de aplicações, da otimização da organização física dos dados em bases de dados, da configuração dos sistemas operativos dos sistemas gestores de bases de dados (SGBD) são exemplos de assuntos tipicamente tecnológicos da área das TI (Pereira, 2005, p. 24).

O mero investimento nas TI conjugado com a sua simples utilização, não se devem esperar vantagens competitivas, pois a grande questão que se coloca às organizações prende-se com a gestão das tecnologias (Strassman cit. por Almeida, 2011, p.6).

Num processo organizacional evolutivo, os SI e as TI desempenham um papel fulcral na gestão da atividade das organizações, e no apoio ao seu processo de decisão, em especial numa época de recursos escassos, em que é fundamental incrementar a eficiência organizacional, rentabilizando recursos humanos, materiais e financeiros.

¹⁷ O *software* que permite por a funcionar todos componentes do computador (*software* de base), bem como transformar os dados em informações (software aplicacional).

¹⁸ Armazenado em Base de Dados (os dados e as informações).

¹⁹ A forma como as pessoas se agrupam para executarem os procedimentos na recolha, seleção, tratamento, análise e produção de resultados (informação).

²⁰ Elemento humano da organização.



4. Sistemas de Informação Policiais

a. Análise evolutiva em Portugal

Os Órgãos de Polícia Criminal (OPC) Portugueses há muito que demonstram uma grande preocupação com a pesquisa de informações, atividade que ganhou, ao longo do tempo, uma importância estratégica global a nível interno e na relação com os outros OPC, pelo que uma houve necessidade de aperfeiçoamento dos instrumentos de pesquisa que gerou investimentos nos meios humanos e materiais nesta área em todas as Instituições (Almeida, 2008, p. 6).

Ao longo do tempo o sistema de registo de informações criminais sofreu uma grande evolução. “Até 1990, com Decreto-Lei nº 295-A/90 de 21/9, que reviu a LO/PJ (Decreto-Lei nº 458/82 de 24/11), a PJ dispunha do Arquivo Central do Registo de Informações (“ACRI”). Em 1990 o ACRI foi transformado no Registo de Informações e Prevenção Criminal, com o escopo da “realização de ações de prevenção criminal e tratamento, registo e difusão, à escala nacional, das informações relativas à prevenção e à IC”, sendo alimentado com informações da PJ, do MP, dos outros OPC, tribunais e de entidades administrativas (e.g. Direção Geral dos serviços Prisionais DGSP) (Almeida, 2008, p. 7).

Com o advento da generalização das ferramentas informáticas, em meados dos anos 90, as tarefas de registo e pesquisa e cruzamentos de informação sofreram uma verdadeira “revolução”, possibilitando respostas quase imediatas para questões que, alguns anos antes, levavam horas ou dias de pesquisa.

A evolução constante associada à necessidade de compatibilizar o tratamento de informação criminal com a proteção de dados pessoais levou a uma necessidade de regulação dos ficheiros informáticos já existentes na PJ, disciplinando a sua organização e atualização, devendo a recolha de dados pessoais “limitar-se ao estritamente necessário à prevenção de um perigo concreto ou à repressão de infrações penais determinadas”, exigindo-se a distinção entre dados factuais, daqueles que incluíam apreciação. (Almeida, 2008, p. 8).

Com a publicação da Lei de Proteção de Dados Pessoais, houve que disciplinar as BD da PJ. Devido à incompatibilidade do sistema criado com o ano de 2000, foi decidido implementar um novo sistema de tratamento de dados que suprisse as necessidades operacionais e estratégicas da PJ, bem como de outras entidades integradas no Sistema de Justiça Nacional, e que se designou por Sistema Integrado de Informação Criminal (SIIC) (Almeida, 2008, p. 9).



A Comissão Nacional de Proteção de Dados (CNPd) indeferiu o pedido de autorização da PJ, considerando que o SIIC, sendo uma base única e de âmbito nacional, carecia de um diploma legal de autorização.

Foi então criada uma comissão para efetuar estudos preliminares com vista à integração da GNR e PSP no SIIC, com aproveitamento do desenvolvimento já operado na PJ. Mais refere Almeida que a PJ alertou a Tutela para a indispensabilidade de harmonizar o sistema, procedendo à regulamentação jurídica de todas essas BD (Almeida, 2008, p. 10).

Em 2006, no âmbito do “Estudo para a Reforma do Modelo de Organização Sistema de Segurança Interna”, do Instituto Português de Relações (IPRI), coordenado é referenciada “a inexistência, na prática, de um sistema de informação criminal, que promova a troca de informações criminais de forma transversal e partilhado de forma simétrica por todos os OPC, aumentada pela separação artificial entre criminalidade de massa e criminalidade organizada, e entre criminalidade doméstica e criminalidade transnacional, que dificulta o reconhecimento do *continuum* atual que se estabelece entre a criminalidade local e global” (Teixeira, et al., 2006, p. 117).

Outra disfunção identificada é a “existência de uma cultura de concorrência institucional entre os vários OPC, constituindo um forte obstáculo à cooperação e coordenação”, bem como a existência de doutrinas táticas, regras de empenhamento distintas, e de níveis de formação e enquadramento diferentes, que dificulta a articulação operacional” (Teixeira, et al., 2006, p. 116).

No domínio particular das informações, o estudo sinaliza “a existência de várias tutelas e multiplicação de FFSS que produzem informações (segurança, criminais e policiais), dificultando a convergência de esforços e potenciando conflitos de competências”, bem como a inexistência de uma cultura de partilha de informações, associada à competição institucional entre as várias FFSS” que tem como consequência “a compartimentação da informação, a inexistência de um fluxo contínuo e eficaz de informações entre serviços de informações e polícias, e vice-versa, e entre as próprias polícias e a duplicação de recursos” (Teixeira, et al., 2006, p. 117).

Relativamente à vertente tecnológica é sublinhada “a falta de interoperabilidade entre as infraestruturas tecnológicas das várias FFSS, com o consequente acréscimo de custos de exploração”.

É ainda apontada a inexistência de uma verdadeira fusão de informações de natureza diversa que potencie a coordenação de esforços e a ação conjunta, nos estritos



limites do Estado de direito, que associada a um entendimento rígido e polissémico do conceito “informações”, gera disfuncionalidade operacional entre informações das polícias e informações dos serviços de informações (Teixeira, et al., 2006, p. 117).

Segundo Portela, as conclusões do relatório supra citado demonstram que o funcionamento do nosso “sistema de informações” sofre de ancilose múltipla, quer pela sua incapacidade interdisciplinar, pela descoordenação entre os vários níveis da administração e entre esta e a sociedade civil, pela inexistência de uma cultura de partilha de informações, pela duplicação de recursos, pela inoperabilidade, pela incapacidade de se autoavaliar e até pela falta de um programa coerente que permita a determinação do significado de “informações” (Portela, 2009, p. 505).

Em 2008, foi aprovada a nova LOIC que retomou a designação “Sistema Integrado de Informação Criminal”, que “assegure a partilha de informação entre OPC, de acordo com os princípios da necessidade e da competência, sem prejuízo dos regimes de segredo de justiça e do segredo de Estado” (AR, 2008).

Finalmente, em 2009, foi aprovada a Lei que estabelece as condições e os procedimentos a aplicar para assegurar a interoperabilidade entre sistemas de informação dos OPC (AR, 2009), aprovando os procedimentos a aplicar para a implementação da Plataforma Para o Intercâmbio de Informação Criminal (PIIC).

Esta lei estabelece como princípios que: os sistemas de informação dos órgãos de polícia criminal são independentes e geridos por cada entidade competente de acordo com o quadro legal especificamente aplicável, devendo, todavia, ser adotadas todas as medidas necessárias para assegurar a interoperabilidade, com vista a possibilitar a partilha de informação através da plataforma; os elementos dos órgãos de polícia criminal e as autoridades judiciais devidamente autorizados têm acesso a informação criminal contida nos sistemas de informação em relação às matérias que, cabendo no âmbito das respetivas atribuições e competências, tiverem, em cada caso, necessidade de conhecer; o fornecimento de dados e informações deve limitar -se àquilo que for considerado relevante e necessário para o êxito da prevenção ou IC **no caso concreto**.

b. Os Sistemas de Informação Policiais em Portugal

Na análise dos Sistemas de Informação (SI) policiais e criminais em Portugal, deveremos ter em consideração que os diplomas legais enquadrantes da atividade, Lei de Segurança Interna (LSI) e Lei da IC (LOIC), bem como das leis orgânicas das FFSS (nomeadamente GNR, PS), PJ, SEF), expressam de modo claro, repetida e inequivocamente a necessidade da implementação da coordenação e partilha da



informação entre as FFSS, em função dos princípios da necessidade e da competência. A interoperabilidade entre os sistemas de informações e acesso a esses sistemas constitui-se num desiderato indispensável para orientar toda a ação policial em função do interesse dos cidadãos (SSI/GTAJ, 2009, p. 2).

A informação recolhida pelos OPC, nessa qualidade, “...através de meios excepcionais que apenas podem ser utilizados, por força da lei, para os fins do processo penal não devem, sem autorização legal expressa, em caso algum ser encaminhadas para outros fins, sejam eles de polícia em sentido estrito, de informações ou de defesa”. Pretendeu assim o legislador estabelecer uma clara distinção entre organismos judiciais e policiais, por um lado, e os Serviços de Informações por outro (que já referimos supra), com o intuito de evitar abusos ou ilegalidades, em pleno respeito pela Constituição da Republica Portuguesa (CRP) (SSI/GTAJ, 2009, p. 3).

A caracterização dos SI das principais FFSS que compõem o Sistema de Segurança Interna Português encontra-se descrita em apêndice 3.

c. A adequação dos SI à AC

A questão da adequação dos SI à AC foi alvo da 5.^a questão colocada aos entrevistados. A resposta, regra geral, foi no sentido da inadequação dos SI ao trabalho do analista tendo sido apontadas diversas disfunções nos Sistemas que seguidamente se espelham.

O trabalho de AC, no âmbito tecnológico, assenta e decorre do emprego de duas ferramentas essenciais: “bases de dados”²¹ (leia-se SI), preferencialmente um repositório único (ou uma plataforma integrada, diremos nós), contendo toda a informação necessária a cada análise; e, para relacionar elevados volumes de dados, ferramentas tecnológicas de análise (e.g. i2, iBridge, iBase,) (Pereira, 2013) refira-se a este propósito que na GNR, a título de exemplo, o SIIOP não está ainda estruturado para que os *outputs* possam dar uma resposta às reais necessidades da AC (operacional e estratégica), a informação inserida no sistema tem constrangimentos ao nível da pesquisa e edição pelos analistas, não permitindo os resultados desejáveis (Branco, 2013) estando em re-análise o desenho funcional do SIIOP, com vista à correção de algumas das suas funcionalidades.

²¹ Em diversos pontos das entrevistas os elementos entrevistados se referiram a “Bases de Dados” (BD), referindo-se aos SI, como supra explicitado, pelo que a bem da clarificação conceptual seguida ao longo deste trabalho substituiremos, onde se justifique, as BD por SI.



Como refere Gomes, existem três grandes problemas com qualquer SI: o primeiro é a qualidade da informação inserida, o segundo é relacionar o que existe e o terceiro é a disponibilização final da informação.

Relativamente à qualidade da informação inserida, constata-se a existência de um conjunto vasto de campos que não são, na prática, em muitos casos, preenchidos (Gomes, 2013) e, mesmo admitindo que possa não haver informação inicial disponível, quando a mesma é recolhida durante a investigação o registo já não é completado. Neste particular sublinha-se ser essencial existirem níveis de controlo da qualidade da informação inserida (em todos os SI) e formação e alerta permanente, instituindo uma cultura de responsabilidade nos elementos que “alimentam” os SI.

Quanto ao relacionar da informação, o problema coloca-se pela dificuldade de ligar a informação (e.g. nomes, números de telefone, moradas, viaturas...) dispersa em diversos campos, não sendo possível estabelecer ligações a outros elementos/processos (Gomes, 2013), este problema que existe em cada sistema, aumenta exponencialmente quando tratamos a partilha entre SI.

O terceiro aspeto a ter em conta é a disponibilização da informação em tempo útil, entre SI a que os OPC acedem, próprios ou protocolados. Dadas as diferenças conceptuais desses SI, o acesso é limitado. Para ultrapassar estas questões têm de ser definidas plataformas compatíveis, criando a possibilidade de cruzamento de dados e a sua disponibilização com mecanismos automatizados e regulamentados (Gomes, 2013).

Noutra perspetiva, Rocha elabora uma asserção crítica no que respeita aos SI policiais internacionais (e.g. EUROPOL e INTERPOL), concluindo que são demasiados, com informação redundante, diferentes formas de acesso e com procedimentos muito burocratizados, o que dificulta a sua operacionalização e o consequente trabalho dos analistas (Rocha, 2013).

Como refere Vieira, os SI policiais nunca serão perfeitos, carecem de permanente adequação à realidade e de melhorias com a introdução de novas metodologias. É muito importante estar atento a outros procedimentos técnicos, em especial os que são aplicados por forças de outros países (Vieira, 2013), acrescentaremos que em época de escassez de recursos se torna essencial rentabilizar mecanismos existentes e criar sinergias para implementar projetos futuros, numa lógica integrada.



d. A Interoperabilidade entre SI e a partilha de Informação Criminal

A partilha de informação criminal entre as FFSS, na qualidade de OPC é uma realidade, embora, por regra, dependa de atos de vontade de quem a detém, o que, só por si é limitativo (Cruz, 2012). O que não existe é uma partilha através de um Sistema Integrado de Informação Criminal, isto é, o verdadeiro SIIC, que como suprarreferido, o legislador “estabeleceu” nas LOIC de 2000 e de 2008, mas “nunca o conseguiu criar”. A inexistência de um SIIC limita muito a quantidade e, principalmente, a qualidade da partilha de informação entre os OPC, mas também no que respeita ao relacionamento entre os OPC e as Autoridades Judiciárias, no âmbito das investigações de um inquérito em concreto (Pereira, 2013).

A partilha de informação criminal ocorre de forma tempestiva, com processos burocratizados a nível dos pedidos e respostas, com recurso a suportes de transmissão desajustados e pouco céleres e sem que exista um conhecimento efetivo da informação que cada um das FFSS possui (Rocha, 2013).

A cultura organizacional dos OPC constitui-se num obstáculo à partilha, “a velha questão de querer saber os o que os outros sabem mas não querer que os outros tenham conhecimento do que eu sei ... está tão presente hoje como há vinte anos”. Mesmo nos canais privilegiados de troca de informação, sejam grupos de trabalho ou acordos oficiais, a partilha é efetuada “ponto a ponto”, através de pedidos de pesquisa e está presente o princípio de “só dou se não me for desfavorável” (Gomes, 2013).

Santos considera a este propósito que a adequada formação do elemento humano das organizações, criando uma cultura de trabalho de equipa, são fatores críticos de sucesso (Santos, 2013). Na essência tudo assenta tudo assenta nas “pessoas” e na sua predisposição para a partilha (Fernandes, 2013), acrescentaríamos que tudo assenta na liderança, que como vimos acima, é o pressuposto fundamental em qualquer sistema de ILP.

e. A Plataforma Para o Intercâmbio de Informação Criminal PIIC

Relativamente a esta questão, os entrevistados consideraram, regra geral que a implementação da PIIC permitirá a ganhos ao nível da partilha informação criminal e, conseqüentemente, da análise de informação criminal, quer numa perspetiva estratégica, quer operacional, bem como para a melhoria da IC, tendo contudo sido apontados “virtudes” e “defeitos” ao sistema em implementação.

Quando às “virtudes” assinaladas, será de referir que, como refere Vieira se trata do primeiro grande passo para o intercâmbio de informação criminal que vem potenciar o



trabalho dos elementos policiais afetos à atividade de AC e auxiliar o desenvolvimento das tarefas inerentes à IC ao permitir a congregação e a interoperabilidade dos SI das várias FFSS, algo nunca antes operacionalizado (Vieira, 2013), e em alinhamento com as recomendações da UE relativamente à interoperabilidade dos sistemas de informação, decorrentes das decisões de PRUM e da própria estratégia de Estocolmo (Nascimento, 2013). Irá ainda permitir adquirir o conhecimento necessário à evolução qualitativa futura do próprio sistema (Pereira, 2013).

Primeiro, refira-se que a plataforma atualmente em implementação fica aquém daquilo que seria ideal, um “verdadeiro SIIC” que o legislador (LOIC) de 2000 e de 2008 parecia pretender implementar, para assegurar a partilha de informação criminal, indo além da atual Lei nº 73/2009, de 12 de agosto. E, segundo Pereira, era essa também a vontade dos responsáveis máximos da GNR, da PSP e da PJ, como decorre do Projeto PIC (Projeto de Partilha de Informação Criminal).

Para Gomes, o sucesso da plataforma vai depender do modo como for efetivamente implementado, apresentando algumas limitações, como a necessidade de contactar o OPC em concreto e de, eventualmente, ter de recorrer ao MP para o acesso a informação sinalizada na PIIC, podendo ser uma mais-valia para trabalhos planeados, mas não para situações que carecem de resposta rápida (Gomes, 2013).

De igual modo, Marques sublinha a limitação que informações que não se encontrem associadas a inquéritos, mas que possibilitariam iniciar novas linhas de investigação e/ou associar/ligar outros suspeitos, não irão estar disponíveis por esta via (Marques, 2013), acresce referir que se tratando apenas de partilha de informação criminal e não de informações, invalida, por exemplo, pesquisas para efeitos “meramente” preventivos (Cruz, 2013).

f. Perspetivas de evolução dos SI

Para responder aos desafios que se colocam à segurança no presente e no futuro, exige-se às FFSS uma constante capacidade de atualização de metodologias de ação e inovação da componente tecnológica, associada a uma cooperação (policial e judiciária), a formação adequada e contínua dos investigadores/analistas, a disponibilidade de meios e a partilha (“desinteressada”) de informação, por quem de direito, como forma de enfrentar fenómenos criminais de crescente complexidade.

Os caminhos para o melhoramento dos SI policiais e criminais passam, forçosamente pelas melhorias de âmbito organizativo, pela formação e qualificação dos



recursos humanos, pela interoperabilidade entre SI das FFSS, quer nacionais (essencial) quer internacionais, bem como por dotar as estruturas de AC com ferramentas tecnológicas de análise especializadas (I2, IBridge, IBase, SPSS) e outras que permitam permitindo o cruzamento de informação georreferenciada, bem como as plataformas de acesso e de análise de fontes abertas (incluindo a capacidade de análise aprofundada das redes sociais). Refira-se ainda a necessidade essencial de especializar cada vez mais os analistas, ministrando-lhe a adequada formação e possibilitando o seu desenvolvimento pela experiência e partilha de conhecimentos.

A nível doutrinário será essencial a criação de uma verdadeira cultura de informações (nacional). A ILP só pode ser verdadeiramente operacionalizada com preceitos e princípios doutrinários comuns (como sucede no RU, nos EUA e outros países), onde um número e uma diversidade muito superior de FFSS efetuam um esforço de uniformização e de partilha que, num país de pequena dimensão como Portugal deveria ser simples mas, fruto de inúmeras resistências, se torna tá difícil de operacionalizar.

É essencial incrementar a cooperação policial, (e judiciária) e operacionalizar a “desburocratizar” as trocas de informação a nível internacional. Num espaço sem fronteiras só o esforço conjunto pode resultar no combate á criminalidade judiciária a nível

A adoção de soluções tecnológicas de georreferenciação vão pois facilitar o trabalho do analista da compreensão de fenómenos, permitindo-lhe entre vários aspetos circunscrever a sua amplitude (locais, regionais, nacionais e transnacionais), conhecer as áreas de atuação de indivíduos e/ou de grupos (locais e/ou itinerantes), apresentar propostas de articulação operacional ou de medidas preventivas (Fernandes, 2013; Cruz, 2013) A Guarda dispõe do SIG-SIRESP, ferramenta que foi desenvolvida para o comando e controlo dos elementos policiais sendo de elevado nível tecnológico e que poderia ser interligada com os SI criminais promovendo a georreferenciação dos fenómenos.

É preciso “investir” no conhecimento que pode ser providenciado pelas universidades portuguesas promovendo protocolos com as FFSS. Há imenso potencial pode ser canalizado na criação de soluções tecnológicas que maximizem o trabalho de análise e de produção de informações, tal como o desenvolvimento de soluções inovadoras no âmbito dos SI. Os analistas, melhor do que ninguém, podem funcionar como consultores na criação de soluções tecnológicas. Eles conhecem as suas necessidades diárias e as suas ideias podem pois ser experimentadas e trabalhadas por quem tem conhecimentos técnicos (Fernandes, 2013).



Reportando-nos ao nível político e estratégico das FFSS, temos de sublinhar a suprema importância (principalmente num período de escassez de recursos) a execução de um Plano Estratégico de Sistemas de Informação (PESI) policial, ao nível tutela, bem dimensionado e exequível, resultante de uma avaliação parcelar de cada Força e Serviço sendo vertida num plano tecnológico próprio. Neste âmbito, verifica-se amiúde que não há alinhamento de conceitos, de doutrina, ou mapeados “processos de negócio”. As organizações têm que ter uma visão sistémica sobre SI. Há que “organizar ideias”. Por exemplo, deveremos falar de um único Sistema de Informação Policial? Ou antes num ecossistema informacional em que o ativo “informação” e as suas “dimensões de qualidade²² mencionadas por “Laudon” no seu livro *“Information management Systems”* deverão ser asseguradas a todo o custo, através de “dicionários de dados” ou de metadados bem inventariados entre os vários SI de entidades que devam colaborar entre si, permitindo assim que os seus sistemas proprietários possam ser interoperáveis ou integráveis (Santos, 2013).

A evolução destes aspetos permitirá melhorar a eficiência decorrente de atividades de produção de informação, tanto no âmbito das informações criminais como das IP.

²² Fiabilidade, Coerência, Consistência, Completude, Validade, Oportunidade e Acessibilidade



Conclusões

As sociedades modernas são caracterizadas por um esbatimento entre a segurança interna e a externa dos Estados, nomeadamente nas ameaças mais gravosas como o terrorismo ou a criminalidade altamente organizada e transfronteiriça, que leva a reequacionamento dos meios adequados para as enfrentar.

Os fenómenos criminais têm vindo a acompanhar essa evolução da sociedade globalizada, atingindo novos patamares de complexidade e sofisticação, com características transnacionais, constituindo um forte desafio para os Estados em geral, e para as FFSS, em particular. O confronto com estas realidades criminais, potenciadas pela facilidade de movimentação de pessoas e bens, a nível global, devido a uma rede de transportes fluida e pela abertura de fronteiras, bem como a uma vertiginosa evolução tecnológica ao nível das comunicações, tem que ser encarado numa perspetiva de coordenação de esforços, quer internacionalmente, quer entre os atores dos sistemas de segurança nacionais. Por outro lado, a exploração das redes informáticas das quais as sociedades dependem em elevado grau para as atividades correntes, mas que se constituem num espaço privilegiado para as atividades ilícitas e de cariz criminal, constitui-se também num problema de segurança emergente.

No espaço europeu surge aquilo que António Vitorino denomina como “ordem pública Europeia”, associada não apenas à criminalidade organizada ou à criminalidade itinerante transnacional, mas também a fenómenos como o “holiganismo” ou os grupos extremistas e radicais “antiglobalização”, fatores que exigem a colaboração entre estados, a nível policial e dos sistemas de justiça, e que tem tido resposta na implementação de projetos como a INTERPOL, a EUROPOL ou o EUROJUST, bem como o Sistema de informação Schengen. A cooperação não sendo perfeita, vai avançando movida pela necessidade, sobretudo no âmbito dos SI, embora os sistemas jurídicos sejam diferenciados.

A nível interno, os Estados enfrentam desafios enormes para a manutenção da segurança coletiva. Em Portugal, por regra, a cooperação surge como um processo difícil, apesar de as normas jurídicas não serem um obstáculo, com acontece entre estados. Tendencialmente as organizações policiais adaptam-se mais lentamente do que as organizações e os indivíduos que se dedicam ao crime, carecendo de condições para enfrentar estes novos desafios da modernidade criminal. É fundamental passar de estruturas baseadas num elevado número de meios humanos (até fruto das restrições materiais a que os Estados se encontram sujeitos), para uma cada vez maior especialização



e tecnicidade na abordagem dos problemas, apostando em recursos humanos com elevados níveis de formação técnica e científica, em permanente atualização, bem como nas novas tecnologias e métodos de processamento de informação, associados a uma clara necessidade de efetiva cooperação institucional.

Para enfrentarem os desafios enunciados o Estado e as suas FFSS têm obrigatoriamente de desenvolver competências ao nível das informações, passando não apenas pela pesquisa, análise e tratamento da informação disponível, mas também pela sua disponibilização aos elementos que dela realmente necessitam tempestivamente.

Para tal, e reportando-nos especificamente ao caso português, constatamos que a cooperação policial entre as diversas FFSS, ao nível da partilha de informações, carece de uma definição há muito requerida, mas não efetivamente implementada ao nível dos SI policiais. Cada FFSS tem o seu próprio sistema, com características próprias, na maior parte dos casos não interoperáveis e com intercâmbios “ponto a ponto” dependendo da circulação de pedidos de pesquisa e de informação. Será este modelo adequado a enfrentar os graves desafios sumariamente descritos?

Foi este o ponto de partida para a nossa investigação, que conduziu à questão central *“Qual o contributo da análise criminal para a produção das informações policiais e criminais, face aos sistemas de informação implementados em Portugal?”*

Tendo surgido a necessidade de balizar a nossa investigação procedemos à definição de um conjunto de hipóteses e elaborámos diversas perguntas derivadas, às quais procurámos responder com o escopo final de esclarecer e definir a resposta à pergunta de partida formulada.

a. Resposta às questões derivadas

(QD1) – Serão as informações um importante pilar da atividade policial na atualidade?

As IP constituem o produto de um processo analítico que avalia a informação recolhida de diversas fontes, integra a informação relevante num produto consistente e produz uma conclusão ou estimativa sobre os fenómenos criminais através de uma perspetiva orientada para a resolução de problemas. As IP são um produto sinérgico que visa providenciar orientações significativas e confiáveis aos decisores policiais sobre criminalidade complexa, organizações criminais, extremistas e terroristas, mas também



sobre o crime comum, para a detenção dos suspeitos ou autores, para proteger possíveis alvos e criar estratégias para eliminar ou reduzir as ameaças.

As IP são também a base para a condução das operações e para possibilitar o uso eficiente dos recursos policiais, através da criação de estratégias de atuação, bem como para a condução com sucesso das ações de IC.

(QD2) – Qual o contributo da AC na atividade policial, de prevenção e IC, bem como para o desenvolvimento de políticas de segurança?

A AC consiste no estudo sistemático dos fenómenos criminais e de situações de desordem, tendo por base fatores sócio demográficos, espaciais e cronológicos, direcionado para fornecer informação pertinentes e atempadas relativamente a padrões criminais e correlação de tendências, visando o desenvolvimento de políticas de segurança (cita-se a título de exemplo os estudos de fenómenos como assaltos a ourivesarias, ou furto de metais não preciosos que geraram alterações legislativas na regulação dessas atividades), mas também o apoio às FFSS na avaliação, prevenção e combate aos eventos criminais e desordens públicas, sendo ainda essencial no quadro do apoio aos investigadores para a resolução de processos-crime.

Em Portugal, de um modo geral a AC é tida como uma vertente essencial ao nível da IC, em geral em todas as FFSS, pois serve de base à decisão estratégica, mas também orienta a aplicação dos recursos ao nível tático, podendo ainda ter um papel na identificação de boas práticas e lições aprendidas, através do estudo da atividade policial em ambos os níveis.

(QD3) – Os SI das FFSS em Portugal respondem às necessidades da análise na produção de informações policiais e criminais?

Constatou-se ao longo do trabalho que a AC poderia ser mais potenciada, se os analistas fossem dotados de acesso a sistemas de informação bem dimensionados às “necessidades de informação” e “contextos de utilização” dos diversos tipos de intervenientes, permitindo que o “conhecimento policial mais geral” sobre os fenómenos criminais que, diretamente ou indiretamente, estão interligados pudesse chegar em tempo a quem dele necessita. Tal não sucede totalmente, porque a informação se encontra espartilhada por SI não compatíveis, sendo a partilha efetuada através de pedidos de informação. Por diversos motivos, de onde se destaca a resistência organizacional e alguma falta de vontade política, o SIIC nunca foi verdadeiramente implementado, estando agora a ser dados os passos para a PIIC que irá ainda apresentar limitações mas que constitui um primeiro passo positivo.



(QD4) – Como podem ser melhorados os SI das FFSS em Portugal para obter uma melhor resposta da AC no contributo para a prevenção e IC?

A adequada formação do elemento humano das organizações, criando uma cultura de trabalho de equipa, é um fator crítico de sucesso. Apesar de a vertente tecnológica não poder ser descurada, para que duas organizações diferentes possam tornar perfeitamente interoperáveis os seus sistemas em termos da sua “cadeia de valor”, deverão estabelecer protocolos de entendimento ao nível dos seus processos de negócio, mapear modelos de dados (dicionário de dados) necessários para transacionar dados, ter aplicações bem dimensionadas e uma infraestrutura tecnológica de suporte adequada (cita-se a necessidade de expandir definitivamente e no curto prazo o SIIOP a todo o TN). Outro aspeto pertinente é a adoção de ferramentas de SIG que comportem a georreferenciação de toda a atividade criminal, bem como a generalização de ferramentas tecnológicas de análise (e.g. Ibase).

O envolvimento das lideranças é essencial para uma adequada implementação das capacidades de análise nas FS, através da demonstração de que há ganhos relevantes de custo benefício para as Instituições, nomeadamente viabilizando criação de uma doutrina única de informações, à semelhança do que se verifica noutros países (e.g. NIM Britânico, ou até na EUROPOL, a nível europeu).

b. Teste das Hipóteses

Passamos assim testar as hipóteses apresentadas

H1: A atividade das FFSS carece de informações que suportem o processo de decisão policial e as atividades de prevenção e de IC.

Ao longo do trabalho constatámos que esta hipótese foi validada por se verificar que quando incidem sobre questões de segurança, as *informações* visam prevenir a existência de circunstâncias propícias à prática de crimes ou à quebra da ordem e tranquilidade públicas, sendo que no âmbito estratégico têm como destinatários os órgãos de decisão política ou as chefias de topo das autoridades policiais. Acresce que o conhecimento se constitui um fator estratégico na gestão operacional das FFSS, nas mais diversas áreas de atuação, e as informações guiam necessariamente a ação policial.

Verifica-se também que informações se constituem como elemento fundamental para a IC visando confirmar evidências, indícios e obter conhecimentos sobre a atuação criminosa, bem como a identificação de redes e organizações que atuem no crime



contribuindo para a descoberta da verdade material e para a conservação de meios de prova.

H2: A AC é um fator crítico para o planeamento da atividade policial e para a IC, bem como para a implementação de políticas públicas de segurança.

A hipótese foi validada pelo nosso estudo, constando-se que a AC é a chave que liga os eventos, os problemas e as respostas, possibilitando uma estratégia coerente das FFSS, sendo responsabilidade primária do analista providenciar a informação necessária para suportar o processo de decisão. Verifica-se que os campos em que AC pode ser usada são vastos e incluem: a resolução de processos-crime; a detenção de criminosos; o desenvolvimento de estratégias e táticas para a prevenção do crime; o estabelecimento de melhorias na segurança da atuação policial, entre outros.

Considera-se que o desenvolvimento do papel dos analistas de atividade criminal poderá constituir-se num multiplicador de capacidade na melhoria da segurança pública, reduzindo os índices de criminalidade e incrementando a segurança da sociedade.

H3: Os SI policiais existentes em Portugal são adequados enquanto instrumentos de suporte da AC e da produção de IP.

Esta hipótese foi apenas parcialmente validada, pois dentro das FFSS os analistas efetuam a AC com os SI de que dispõem, cujo grau de qualidade no fornecimento da informação varia de SI para SI, elaborando produtos com algum grau de qualidade. Por outro lado, em muitos casos não possível perceber a realidade total dos fenómenos criminais, por diversas lacunas que os SI apresentam e porque a informação se encontra dispersa e não compatibilizada, inclusive do ponto de vista estatístico. Desde seria necessário um repositório que agrupasse ou partilhasse toda a informação disponível. Depois acresce que na GNR, por exemplo, o SIIOP não cobre a totalidade do território, o que constitui uma séria limitação e que na PJ foi apontada a dificuldade de cruzamento de todos os dados disponíveis. Além disso há muitas lacunas quanto ao controlo da qualidade da informação inserida, acrescentando que nenhum dos sistemas permite a georreferenciação do crime.

H4: A interoperabilidade entre SI e uma efetiva partilha de Informações são indispensáveis para garantir o funcionamento eficiente da AC nas FFSS em Portugal.

A hipótese é validada considerando-se que apurámos ao longo do trabalho que a cultura organizacional dos OPC constitui-se, não raro, num obstáculo à partilha, pelo esta ocorre de forma tempestiva, com processos burocratizados a nível dos pedidos e respostas,



com recurso a suportes de transmissão desajustados e pouco céleres e sem que exista um conhecimento efetivo da informação que cada um das FFSS possui

Ressalta ainda a falta de formação base comum e a inexistência de um sistema e/ou procedimentos técnicos idênticos, sendo que as diferentes competências funcionais e a importância que cada Organização atribui à área da Informações, que acaba por ser um obstáculo. É fundamental implementar a PIIC e fazê-la evoluir comportando outros tipos de informação relevante, que não apenas a constante de processo crime, como atualmente acontece.

c. Resposta à questão central

Recordamos aqui a questão central do nosso trabalho, à qual procuraremos responder, concluindo assim o nosso percurso investigatório.

“Qual o contributo da análise criminal para a produção das informações policiais e criminais, face aos sistemas de informação implementados em Portugal?”

A análise estratégica, enquanto instrumento de apoio policial no âmbito interno de cada FFSS, contribui para a tomada de decisão estratégica e para a implementação de políticas de prevenção criminal. A cabal compreensão dos fenómenos criminais, mediante as mais diversas metodologias de AC, permite orientar o esforço das subunidades policiais na aplicação de medidas preventivas e de cariz operacional, como sejam, ações direcionadas para locais específicos e/ou indivíduos/grupos suspeitos, pela identificação de MO, que no conjunto permitirão o direcionamento do patrulhamento e o estabelecimento de prioridades, definir o perfil das vítimas (permitindo a adoção/recomendação de medidas passivas e ativas direcionadas) e também de identificar zonas de maior incidência de atividade criminal, possibilitando assim, também, a mais racional distribuição de meios.

Cita-se a título de exemplo a emergência de “novos fenómenos” criminais, como o furto de caixas multibanco, o furto de metais não preciosos, ou os fenómenos de “*carjacking*”, cujo impacto do seu estudo gerou uma quase “obrigatoriedade institucional” de monitorar as ocorrências e perceber as dinâmicas dos indivíduos/grupos associados, a comunicação com as diferentes Instituições policiais (nacionais e internacionais) e não policiais (SIBS e entidades bancárias, associações de empresários), com vista à congregação de esforços que funcionassem como alerta e travão ao crescente número de delitos praticados e, inclusive, a alterações legislativas em diversos âmbitos (e.g. criminalização da prática do crime de casamento ou união de conveniência ou a alteração ao regime do controlo dos operadores de resíduos, nos estudos sobre o furto de metais não preciosos).



Cita-se ainda o contributo para as decisões sobre as políticas no domínio da segurança interna (e.g. Lei sobre Política Criminal e Plano de Coordenação, Controlo e Comando Operacional das FFSS) e para a adequada implementação dessas políticas.

Verifica-se contudo que estas medidas têm geralmente uma vertente mais reativa aos fenómenos, que vão evoluindo, do que a desejada proatividade, no âmbito da tomada de decisão estratégica, dado que mesmo quando geram alterações são, geralmente, uma consequência da evolução dos fenómenos e não os antecipam, como seria expectável.

Ao nível da investigação criminal existem níveis diferentes de avaliação da informação que contribuem para a eficácia do processo investigatório, sendo efetuado um acompanhamento, num processo de análise operacional, em paralelo à investigação, com especial enfoque em análises de caso e de grupos de autores, dependendo da tipologia do crime, geralmente ao nível das investigações mais complexas, tendo em conta que os recursos “analistas” são escassos para as necessidades.

Outra atividade relevante é a monitorização das ocorrências criminais que é efetuada em todas as FFSS, embora com diferentes amplitudes e resultados, dadas as especificidades funcionais e competências, mas que focam, no essencial apenas os fenómenos mais relevantes, como os de impacto transregional e transnacional (e.g. criminalidade violenta e grave, nomeadamente roubos com arma de fogo, crimes sexuais, criminalidade informática, tráfico de droga, burlas...).

O manancial de informação difundido é, geralmente, canalizado para o dispositivo, sob a forma de relatórios, com o objetivo de contribuir para o desenvolvimento das investigações em curso e para a adoção de medidas preventivas de carácter operacional, sendo que esses documentos são muitas vezes alvo de partilha entre as FFSS, havendo inclusive trocas céleres de informação em tipologias criminais previamente estabelecidas.

Assim, verifica-se que a análise criminal em Portugal, produz mais-valias e resultados relevantes na generalidade das Forças e Serviços de Segurança, quer na perspetiva estratégica de apoio à decisão política, quer através dos Relatórios de Informações Criminais que são difundidos ao Dispositivo e que produzem efeitos operacionais assinaláveis no combate a fenómenos emergentes, ou ainda no apoio aos investigadores, em sede de inquéritos criminais, conduzindo à descoberta da verdade e levando à clarificação do percurso investigatório e à produção da prova.

Convém assim sublinhar o esforço, por vezes autodidata, e a dedicação destes profissionais, que trabalham, não raro, sem a formação mais adequada e na ausência de ferramentas especializadas.



Ora, sendo a análise a pedra angular de todas as modernas atividades policiais, “*intelligence led*” e sendo crucial para todas as atividades policiais em organizações em que as capacidades analíticas assentem em tecnologias avançada adaptadas às necessidades da segurança e ordem pública.

Contudo, verifica-se que os SI apresentam, no seu todo, fragilidades estruturais (e estruturantes) pelo fato de terem uma cobertura reduzida no território nacional, não havendo nenhum sistema que contenha a totalidade da informação criminal (e no caso da GNR, nem todo o Dispositivo está coberto, sendo essencial que seja promovida a essencial decisão política para a implementação efetiva do Sistema).

Depois foca-se a questão dos SI não serem efetivamente interoperáveis, ou compatíveis, levando a que as componentes qualitativa e quantitativa (estatísticas) da análise não detenham, em qualquer das FFSS acesso a toda a informação, obrigando a recorrer a pedidos avulsos, com elevado encargo operacional e perdas acentuadas de informação, de tempo e de eficiência no trabalho dos analistas.

Constata-se assim que em Portugal, contrariamente ao que sucede noutros países, não será possível implementar uma verdadeira ILP, enquanto não existir um verdadeiro SIIC, que permita deter uma “imagem” completa da criminalidade, apurando as suas características, causas e incidências, criando estratégias nacionais de emprego eficiente e coordenado dos meios disponíveis e orientando efetivamente o esforço policial de um modo coerente. Para tal, como referiu Bratton (Bratton & Kelling, 2006, pp. 6-8), são necessários três fatores essenciais: tecnologias, formação e, mais importante, liderança efetiva.



Bibliografia

- Almeida, R., 2008. Sistema Integrado de Informação Criminal e Coordenação Policial - Perspetiva Histórica e Jurídica - Conferência na EP GNR Queluz. In: *Interoperabilidade Entre Os Sistemas De Informação De Entidades Que Fazem Parte Do Sistema De Segurança Interna*. s.l.:SSI GTAJ, pp. 6-12.
- AR, 2004. *Lei Orgânica n.º4/2004, de 06 de Novembro, Altera e Republica a Lei Quadro do SIRP*. s.l.:DR.
- AR, 2007. *Lei n.º 9/2007, de 19 de Fevereiro, Estabelece a orgânica do Secretário-Geral do SIPR, do SIS e do SIED*. s.l.:DR.
- AR, 2008. *Lei 49/2008 de 27 de Agosto, Lei de Organização da Investigação Criminal*. Lisboa: DR.
- AR, 2008. *Lei Lei n.º 53/2008, de 29 de Agosto - Aprova a Lei de Segurança Interna*. s.l.:DR.
- AR, 2009. *Lei 73/2009, de 12 de Agosto (Define a Interoperabilidade entre sistemas de informação dos órgãos de polícia criminal)*, Lisboa: DR.
- AR, 2009. *Lei n.º 38/2009, 20 de Julho*. Lisboa: DR.
- Bagina, F., 2009. Polícia De Segurança Pública: S.E.I - Sistema Estratégico De Informação. In: *Interoperabilidade entre os sistemas de informação das Entidades que fazem parte do Sistema de Segurança Interna*. GTAJ. Lisboa: SSI, pp. 28-38.
- Bessa, J. S., 2004. A Importância da Inteligência no Processo Decisório. In: C. C. Ltda, ed. *Encontro de Estudos: Desafios para a Atividade de Inteligência No Século XXI*. Brasília: Gabinete de Segurança Institucional, Secretaria de Acompanhamento e Estudos Institucionais, pp. 51-71.
- Borges, M., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (17 04 2013).
- Branco, C., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (17 04 2013).
- Bratton , W. J. & Kelling, G. L., 2006. Policing Terrorism. *Civic Bulletin*, 43.
- Cardoso, P., 2004. *As Informações em Portugal*. 1.^a ed. Lisboa: Gradiva / IDN.



Carter, D. L., 2004. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies. School of Criminal Justice.* Michigan: Michigan State University.

Christopher, B., 2008. Fundamentals of Crime Analysis. In: S. L. e. a. Gwinn, ed. *Exploring Crime Analysis.* South Carolina: IACA - International Association of Crime Analysts, pp. 7-32.

Clemente, P. L., 2006. *A Polícia em Portugal - Cadernos do INA n.º 26,* Oeiras: Instituto Nacional de Administração.

Clemente, P. L., 2008. *As Informações de Polícia - Palimpsesto.* Lisboa, Instituto Superior de Ciências Policiais e Segurança Interna.

Cruz, A., 2012. *Órgãos De Polícia Criminal: Um Modelo Para Portugal. Trabalho de Investigação Individual do Curso de Estado Maior Conjunto,* Lisboa: Instituto de Estudos Superiores Militares.

Cruz, A., 2013. *Análise Criminal e Sistemas de Informação [Entrevista] (17 04 2013).*

Dantas, G. & Souza, N., 2004. *As bases introdutórias da análise criminal na inteligência policial - Seminário de Inteligência e Criminalidade de Massa (15 e 16 Julho).* Brasília, Agência Brasileira de Inteligência - ABIN - portal.mj.gov.br.

Delpeuch, T. & Scheeffter, T., 2013. *Developing local security intelligence in German and French police forces - Bringing together two knowledge cultures through the CODISP project.* [Online]

Available at: http://www.agence-nationale-recherche.fr/Colloques/WISG2013/presentations/AAP11_CODISP.pdf

[Acedido em 11 03 2013].

Elias, L., 2012. Desafios à Segurança numa sociedade globalizada. *Observatório Político - working paper 11,* maio.

EUROPOL, 2011. *Europol Review - Relatório Geral sobre as atividades da EUROPOL,* Haia: Serviço Europeu de Polícia.

Exército, 2009. *PDE 2-00 -INFORMAÇÕES, CONTRA-INFORMAÇÃO E SEGURANÇA.* s.l.:Exército Português.



FBI, 2004. *Federal Bureau of Investigation, Directorate of Intelligence, Intelligence Cycle*.
[Online]

Available at: <http://www.fbi.gov/about-us/intelligence/intelligence-cycle>
[Acedido em 12 04 2013].

Fernandes, T., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (12 04 2013).

Furtado, V., 2002. *Tecnologia e Gestão da Informação na Segurança Pública*, Fortaleza: Garamond.

Garcia, F. P., 2009. O fenómeno da guerra no nosso século. *Relações Internacionais [online]*, n.º22, pp. 103-120.

GNR, 2012a. *Módulo de Contra Informação e Segurança, Apontamentos do 1.º Curso de Informações da Guarda Nacional Republicana*. Queluz: Direção de Informações / Escola da Guarda.

GNR, 2012b. *Teoria Geral de Informações, Apontamentos do 1.º Curso de Informações da Guarda Nacional Republicana*. Queluz: Direção de Informações / Escola da Guarda.

Gomes, P., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (11 04 2013).

Grenho, J., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (10 04 2013).

Grenho, J. N., 2009. Guarda Nacional Republicana - S.I.I.O.P. - Sistema Integrado De Informações Operacionais de Polícia. In: *Interpreabilidade entre os sistemas de informação das Entidades que fazem parte do Sistema de Segurança Interna*. GTAJ. Lisboa: SSI, pp. 19-28.

Guedes, J., 2010. O sistema Integrado de Informações Operacionais Policiais (SIIOP). *Pela Lei e Pela Grei - Revista da Guarda Nacional Republicana*, Out - Dez, pp. 30-48.

Heuer, R. J., 1999. *Psychology of Intelligence Analysis*. URL: <http://www.cia.gov/csi/books/19104/art9.html> ed. Washington, DC: Center for the Study of Intelligence.

IACP, 2001. *Criminal Intelligence and analysis - International Association Chiefs Of Police*. [Online]

Available at: http://www.oss.net/dynamaster/file_archive/040319/6dac10152ffb23b9de0c3f1334ffca6e/



OSS2001-X1-06.pdf

[Acedido em 12 03 2013].

Lourenço, V., 2006. *Disciplina de Informações, EPP, Módulo 3*. Torres Novas: Escola Prática de Polícia.

Luizio, F. a., 2009. Arquitetura do SIIC da Polícia Judiciária. In: *Interoperabilidade entre os sistemas de informação das Entidades que fazem parte do Sistema de Segurança Interna*. GTAJ. Lisboa: SSI, pp. 13-19.

Marques, F., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (23 04 2013).

Menezes, A. C. d., 2012. *Sistemas de informações nacionais : contributos para a percepção da eficácia - Dissertação de mestrado em História, Defesa e Relações Internacionais*, Lisboa: ISCTE.

Moleirinho, P. E., 2009. *Da Polícia de Proximidade ao Policiamento Orientado pelas Informações - Tese Mestrado em Direito e Segurança, Fac. de Direito, Univ. Nova de Lisboa*, Lisboa: FD UNL.

Nascimento, 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (11 04 2013).

NPIA, 2008. *Practice Advice On Analysis*. Bedfordshire: National Policing Improvement Agency / Association of Chief Police Officers.

Osborn, D., 2006. *Out of Bounds - Innovation and Change in Law Enforcement Intelligence Analysis*. Washigton, DC: Joint Intelligence Military Staff.

OTAN, 2001. *AJP 2.0 (STANAG 2190) Intelligence, CI and security doctrine*. s.l.:OTAN.

Pedro, M. L. M., 2009. O S.E.F. - Serviço de Estrangeiros e Fronteiras. In: *Interoperabilidade entre os sistemas de informação das Entidades que fazem parte do Sistema de Segurança Interna*. GTAJ. Lisboa: SSI, pp. 38-43.

Pereira, A., 2013. *Análise Criminal e Sistema de Informação* [Entrevista] (18 04 2013).

Pereira, J., 2009. O SIRP abriu caminho a um novo rumo para a estruturação da Administração Pública - entrevista. *Revista Segurança e Defesa*, jan-mar, pp. 12-17.

Pereira, M. J., 2005. *Sistemas de Informação: uma abordagem sistémica*. 1.^a ed. Lisboa: Universidade Católica Editora, 2005.



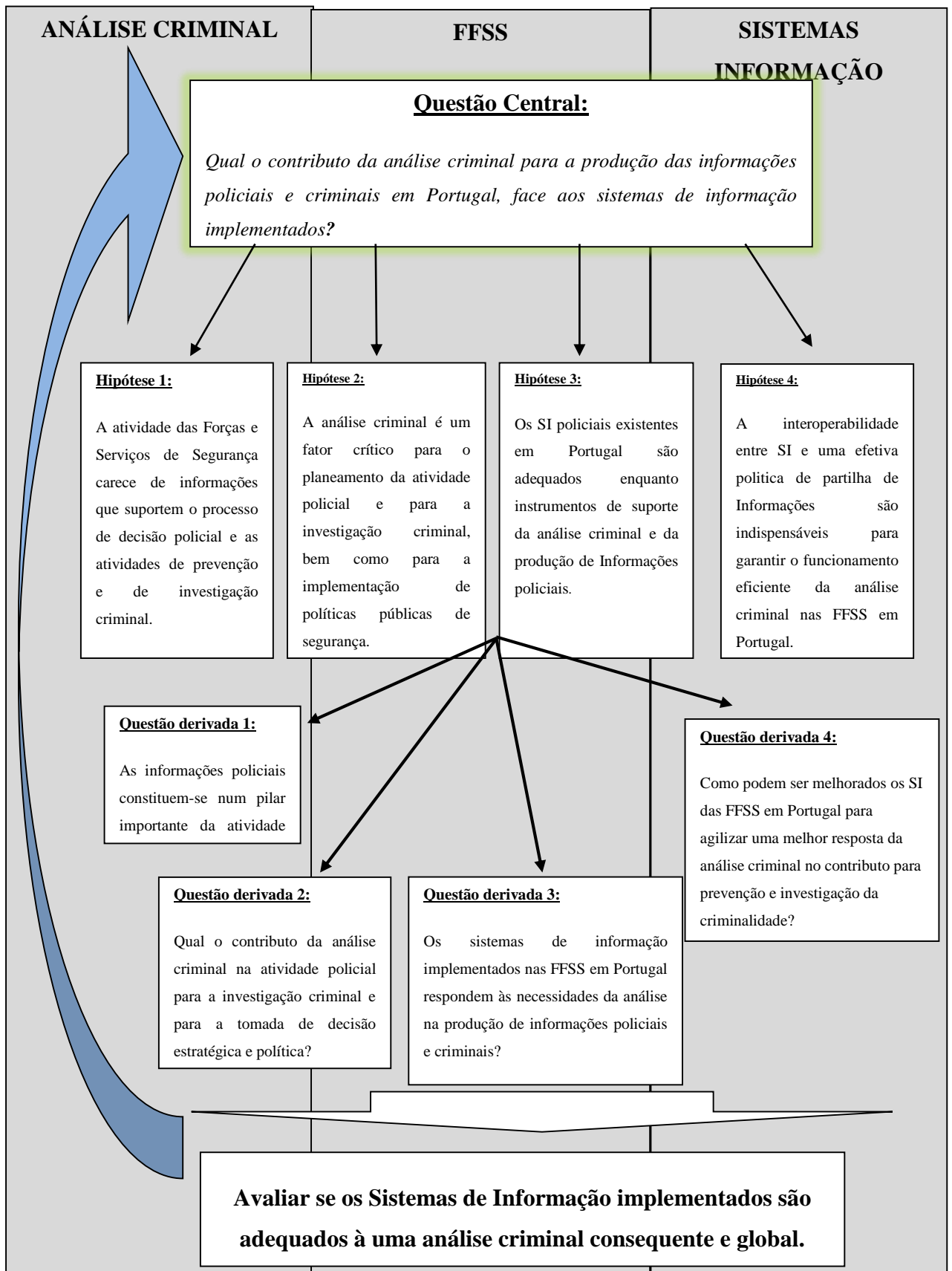
- Pereira, R., 2005. Informações e Investigação Criminal. In: *I Colóquio de Segurança Interna*. Lisboa: Almedina, pp. 155-169.
- PJ, 2010. *Curso de Análise de Informação Criminal*. Loures: Escola de Polícia Judiciária.
- Portela, I., 2009. A segurança interna e o combate ao terrorismo: o caso português. *Revista Enfoques: Ciencia Política y Administración Pública*, vol. VII, núm. 11 - *Universidad Central de Chile*, pp. 491-544.
- Quivy, R. & Campenhoudt, L. V., 1998. *Manual de Investigação em Ciências Sociais*. 2.^a ed. Lisboa: Gradiva.
- Rascão, J., 2004. *Sistemas de Informação para as Organizações*. 2.^a ed. Lisboa: Adições Sílabo.
- Ratcliffe, J. H., 2007. *Integrated Intelligence and Crime Analysis: Enhanced Information for Law Enforcement Leaders*. COPS ed. Washington,DC: Police Foundation.
- Ratcliffe, J. H., 2011. Intelligence-Led Policing. In: *Environmental Criminology and Crime Analysis*. New York: Routledge, pp. 263-283.
- Reis, S. & Silva, M. B., 2007. O Sistema de informações da República Portuguesa. *Revista da Ordem dos Advogados*, ano 67, III - Lisboa (separata)., Dezembro, pp. 1250 - 1304.
- Rocha, Ó., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (17 04 2013).
- Santos, P., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (09 04 2013).
- SSI/GTAJ, 2009. *Interoperabilidade entre os Sistemas de Informação de Entidades que fazem parte do Sistema de Segurança Interna*. Grupo de Trabalho da área Jurídica (GTAJ), Lisboa: SSI.
- SSI, 2008. *Plano de Coordenação, Controlo e Comando Operacional das Forças e Serviços de Segurança*. Lisboa: Sistema de Segurança Interna.
- Teixeira, N. S., Lourença, N. & Piçarra, N., 2006. *Estudo para a Reforma do Modelo de Organização Sistema de Segurança Interna - Relatório Preliminar*, Lisboa: Instituto Português de Relações Internacionais - Universidade Nova de Lisboa.
- Torres, J. M., 2005. A Investigação Criminal na PSP. In: *Estratégia de Gestão Policial em Portugal*. Oeiras: INA, pp. 579-636.



Vieira, A., 2013. *Análise Criminal e Sistemas de Informação* [Entrevista] (10 04 2013).



Apêndice 1 - Linha de Orientação Metodológica





Apêndice2 – Corpo de Conceitos

Informações (*Intelligence*²³)

O processo de tomada de decisão na atualidade de um mundo globalizado e ligado em rede, caracterizado por uma imensidão de dados, divulgados a cada instante pelos órgãos de comunicação social (OCS), ou por outras entidades públicas e privadas, em qualquer parte do planeta, através da internet, carece de informações especiais, necessárias para a melhor condução dos negócios públicos ou privados, e que possam fazer pender, em seu favor, a balança dos eventos futuros, resulta numa crescente importância das atividades de *Informações*. Sherman Kent, no livro “*Strategic Intelligence*” (1967), considera que as *Informações* traduzem “...o conhecimento que um Estado deve possuir em relação aos outros Estados a fim de assegurar que nem sua causa, nem suas iniciativas falhem, devido ao fato dos seus estadistas e soldados planejarem e agirem na ignorância” (Kent, 1967, cit por Bessa, 2004, p. 55).

Já Washington Platt, no seu livro “*Strategic intelligence production*” define *Informações* “...um termo específico e significativo, derivado de informação, fato ou dado, que foi selecionado, avaliado, interpretado e finalmente expresso de forma a evidenciar a sua importância para um determinado problema de política nacional corrente”. Constituindo-se, na perspectiva estratégica, “...no conhecimento referente às possibilidades, vulnerabilidades e linhas de ação prováveis das nações estrangeiras” (Platt, 1957, cit por Bessa, 2004, p. 55).

Para Heitor Romana, o conceito de *Informações* é entendido, em sentido restrito, como “...um processo de obtenção de conhecimento fundamental à tomada de decisão quanto à salvaguarda dos interesses permanentes ou conjunturais dos Estados, assumindo uma natureza e finalidade ofensiva e defensiva” (Romana, 2008, cit. por Menezes, 2012, p. 7). A perspectiva apresentada tem cariz holístico, ou seja, enquanto processo, produto e organização. Relativamente ao processo, Romana, introduz, explicitamente, a ideia de conhecimento que exige um conjunto de atividades, para a sua produção, que vão da manifestação das necessidades, pelo decisor, até à disseminação ao decisor, induzindo uma

²³ Acerca do conceito de *Informações*, deveremos ter em consideração que, na doutrina portuguesa, se usa a palavra informação e o seu plural *Informações* (este para definir o resultado do ciclo de produção de informações - a informação já tratada), correspondendo ao vocábulo anglo-saxónico *intelligence*. Apesar de esta terminologia poder ser geradora de equívocos, pelo que optaremos por colocá-lo em itálico, ao longo do presente, facilitando a explanação e compreensão das ideias que pretendemos transmitir, optámos por nos manter fiéis à doutrina nacional, embora em alguns casos (citações) possamos optar pelo vocábulo inglês, devendo se considerado que têm o mesmo significado.



necessidade de relação biunívoca entre as organizações e decisores. Este processo que decorre na ótica do interesse nacional, exige uma garantia do segredo, pelo que apenas organizações com características próprias permitem atingir este desiderato, constituem-se assim os Sistemas de Informações Nacionais, sob tutela do Estado para prosseguir estes fins (Menezes, 2012, p. 7).

Segundo o “*Dictionary of the United States Military Terms for Joint Usage*”, a “*Intelligence* é o produto resultante da pesquisa, avaliação, análise, integração, e interpretação de todas as informações disponíveis, relativas a um ou mais aspetos de nações estrangeiras ou de áreas de operações e que é imediata ou potencialmente importante para os planificadores”. Já Robert Steele, “*intelligence*” é “a informação trabalhada para dar suporte a uma decisão específica, para uma pessoa específica, sobre um tema específico de um determinado tempo e lugar” (Bessa, 2004, p. 57).

Na aplicação das teorias das *Informações* ao mundo dos negócios encontramos a designada Economia do Conhecimento (*Competitive intelligence*) que pode ser definida como “...o conhecimento do ambiente competitivo da organização e de seu macro-ambiente, aplicado a processos de tomada de decisão, nos níveis estratégico e tático”, segundo John Herring, ou “...as análises sobre o competidor, seus objetivos futuros, sua estratégia atual, e sua capacidade”, segundo Arik Johnson (1998) (Bessa, 2004, p. 59).

Resulta das diversas definições que as funções das *Informações* se inserem numa vasta gama de atividades, quer ao nível governamental, tendo como mote a segurança e as decisões políticas dos governos, quer numa perspectiva empresarial, guiadas pela necessidade de obter vantagens competitivas sobre os concorrentes. Assim, as *Informações* serão o produto acabado (saber e conhecimento), cujo valor advém da eficiente pesquisa de diversas peças de informação, na adequada e profissional integração, análise prospetiva e interpretação das mesmas, e sua rápida e eficaz difusão aos decisores, comportando, sempre que possível, o equacionar de previsões para o futuro.

Contrainformação - é o conjunto de atividades de carácter destinadas a identificar e anular a ameaça proveniente de serviços de informações ou de organizações hostis, ou de indivíduos envolvidos em atividades de espionagem, de terrorismo ou subversão (OTAN, 2001, pp. 2-1-1).

Investigação criminal - segundo Torres, constitui “um conjunto de diligências intelectualmente organizadas metodicamente sequenciadas, realizadas dentro dos limites previstos na legislação em vigor, oportunamente destinadas a apurar a existência dum crime, a descobrir os seus agentes e a esclarecer todas as circunstâncias julgadas relevantes



para a graduação da sua culpabilidade e responsabilidade, para aferição da sua personalidade e para a total delimitação das consequências efetiva ou potencialmente resultantes do ato ilícito”.

Órgão de Polícia Criminal - a designação OPC encontra-se definida no Art.º 1.º do Código de Processo Penal (CPP) como “todas as entidades e agentes policiais a quem caiba levar a cabo quaisquer atos ordenados por uma AJ ou determinados por este Código”. Logo nem todas as FFSS são OPC, como é o caso do SIS, e vários são os OPC que não são FFSS, como a ASAE, sendo que as FFSS, são tuteladas pelo poder executivo (Primeiro Ministro, Ministro da Administração interna (MAI); Ministérios da justiça (MJ); SG/SSI; Ministro da Defesa Nacional (MDN), enquanto os OPC, atuam na dependência funcional do poder judicial (Ministério Público (MP) ou Juiz de Instrução Criminal, “os elementos que não desenvolvem atividades de IC atuam sob dependência hierárquica, enquanto os elementos que pertencem às subestruturas de IC atuam no âmbito do processo, com observância da hierarquia, é certo, mas sob dependência funcional de uma AJ em concreto” (Cruz, 2012, p. 20) Assim. Verifica-se com frequência a utilização do termo OPC e Forças de Segurança ou polícias de modo indiferenciado, o que em nosso entender não é correto

A **prevenção criminal**²⁴ pode ser estruturada em diversas modalidades, em particular a **prevenção clássica**, que visa impedir o cometimento de atos ilícitos (divide-se em: repressão criminal ou prevenção geral²⁵; prevenção situacional²⁶ e prevenção proactiva²⁷); **prevenção psicossociológica**, que “visa contrariar os elementos de natureza

²⁴ Em termos legais, segundo o autor, “constata-se a tendência para o legislador atribuir ou menos admitir competências de prevenção específica e proactiva e até de investigação preventiva aos OPC que sobre as mesmas matérias detêm competências investigatórias e/ou fiscalizadoras [...], organismos que terão o *know how* e a experiência que lhes permite antecipar fatores de risco e descobrir indícios técnicos próprios de determinadas atividades ilícitas”. Residirá neste ponto a justificação para a dispersão de organismos com competências investigatórias específicas.

²⁵ A prevenção geral resulta do efeito conjugado da probabilidade de descoberta dos autores dos crimes, conjugada com a rapidez com que isso sucede e do elemento intimidatório abstrato das penas criminais, que atuam na motivação para delinquir e na expectativa de remuneração passível de ser obtida.

²⁶ A prevenção situacional, obtida através da visibilidade e da presença policial, da “ocupação” de espaços, da proximidade policial, atuando sobre a motivação para delinquir e sobre a vulnerabilidade do alvo.

²⁷ A prevenção proactiva resulta da vigilância e acompanhamento rotineiro de locais, atividades e pessoas de risco obtida através de ações por vezes “intrusivas”, perturbadoras do estado de espírito dos potenciais delinquentes, de natureza controladora e fiscalizadora, atuando sobre a motivação para delinquir e, residualmente, da vulnerabilidade do alvo.

Cita-se o exemplo das rusgas ou operações de fiscalização rodoviária. Nestes casos “a fronteira entre a prevenção e a investigação criminal, especialmente a investigação *pré-processual* ou *pró-activa* função dum objetivo concreto, [...] obtenção de elementos sobre um indivíduo que assume comportamentos suspeitos, típicos de um potencial terrorista”.



socioeconómica, cultural ou meramente conjuntural que potenciam a prática atividades delinquentes ou os seus efeitos perversos, atuando essencialmente sobre as componentes da motivação para delinquir e da atratividade do alvo; **prevenção específica**, “que se baseia na promoção de medidas de autoproteção e de zelo entre as potenciais vítimas de crimes visando reduzir a probabilidade de serem, atuando essencialmente na componente da vulnerabilidade do alvo” (Torres, 2005, p. 586).

Segundo Brandl, a **prevenção criminal** poderá ter outra tipologia traduzida pela: prevenção primária, incidindo nas causas do incidente criminal²⁸, prevenção secundária, que intervém quando o incidente é manifesta²⁹ e pela prevenção terciária que visa evitar a reincidência criminal³⁰ (Brandl, 2004, cit. por Torres, 2005, p. 587).

Resulta assim o equacionar do papel relevante que as IP têm ao nível da prevenção, promovendo o conhecimento atempado da realidade social e criminal e potenciando o direcionar dos meios à disposição dos decisores para as áreas que forem estabelecidas como mais prioritárias potenciando a proteção da comunidade das fontes de perigo mais potencialmente relevantes de perturbação da ordem e tranquilidade públicas (prevenção clássica e psicossocial), mas também das vítimas mais vulneráveis (prevenção específica).

A **ameaça** pode ser definida, no seu conceito tradicional, como “um qualquer acontecimento ou ação (em curso ou previsível), de variada natureza, proveniente de uma vontade consciente e inteligente e que impede a consecução de determinados objetivos; no fundo, o produto de uma capacidade por uma intenção” (Garcia, 2009, p. 5).

²⁸ Passando neste caso forçosamente por políticas sociais, económicas e culturais.

²⁹ Neste caso circunscreve-se aos grupos de risco, abrangendo a prevenção tipicamente a cargo das polícias.

³⁰ A atuação será efetuada sobre a população alvo de sanções criminais ou sujeitas a medidas de segurança.



Apêndice 3 – Trabalho de Campo

Com o objetivo de aprofundar a compreensão sobre as questões em análise e, certificar as respostas que fomos obtendo ao longo do percurso investigatório, com o intuito de alcançar resultados o mais integrais possível para as questões estabelecidas com, tomámos por opção a realização de entrevistas semidirigidas a pessoas com conhecimentos especializados sobre as temáticas em apreço.

Este tipo de entrevistas, a mais utilizada em investigação social, “é semidiretiva no sentido em que não é inteiramente aberta nem encaminhada [...] o investigador dispõe de uma série de perguntas, a propósito das quais é imperativo receber uma informação por parte do entrevistado” deixando que o mesmo fale abertamente pelas palavras que desejar sobre o assunto (Quivy & Campenhoudt, 1998, p. 192).

As questões postas aos entrevistados foram as mesmas, possibilitando a comparação analítica das respostas para a qual elaboramos uma tabela comparativa. Espelhando no trabalho os conteúdos mais relevantes, anexa-se CD contendo as entrevistas integrais.

Caraterização da Amostra

À luz dos objetivos pretendidos procedemos a uma escolha tão criteriosa quanto possível do universo dos entrevistados, baseada nos seus conhecimentos específicos sobre as questões em apreço, nomeadamente nas áreas da investigação criminal, análise criminal, informações policiais e sistemas de informação, tendo em consideração funções relevantes que desempenharam ou desempenham nas FFSS (procurámos entrevistar, pelo menos, um elemento de cada uma das FFSS, com competências policiais) que consideramos mais relevantes no âmbito do SSI, conforme o quadro seguinte:

Entrevistado	Posto	Função Atual	Domínios de Especialização
1	Coronel GNR	Adjunto Comandante Operacional (CO)	Investigação Criminal
2	Coronel GNR	Diretor de Investigação Criminal -	Investigação Criminal
3	Ten. Cor. GNR	Chefe da Divisão - DIC / CO	Investigação Criminal
4	Inspetor PJ	Chefe Análise Criminal PJ	Análise Criminal
5	Sub-Intendente PSP	Coordenador Adj. Gabinete Nacional	Investigação Criminal /
6	Comissário PSP	Oficial de Ligação PSP no Gabinete	Investigação Criminal / Análise
7	Inspetor Ad.	Direção Central de Investigação SEF	Investigação Criminal
8	Coronel GNR	Diretor de Informações - DI / CO	Informações
9	Ten. Cor. GNR	Chefe da Divisão - DI / CO	Informações / SI
10	Ten. Cor. GNR	Chefe da Divisão - DI / CO	Informações / Análise Criminal
11	Ten. Cor. GNR	Chefe de Repartição DI/CO	Informações
13	Major GNR	Chefe de Repartição DCSI / GNR / CO	Sistemas de Informação



Apêndice 3 – Caracterização dos SI das FFSS

(1) PJ

A Polícia Judiciária possui o Sistema Integrado de Informação Criminal (SIIC) que se constitui como uma base de dados única, integrando toda a informação criminal de natureza confirmada e especulativa e que visa otimizar a circulação da informação entre as várias Unidades Orgânicas da PJ, permitindo a coordenação das investigações e a AC (Luizio, 2009, p. 14).

Os conceitos operacionais do sistema baseiam-se na Abertura de Investigação (AI), após a qual são inseridos objetos elementares (fatos, intervenientes e objetos), sendo efetuada uma descrição estruturadas dos crimes. O SIIC permite uma comparação automática dos dados, bem como a coordenação e análise operacional e estratégica da informação contida. O acesso ao sistema baseia-se na necessidade de conhecer e na competência para a investigação e territorialidade, cabendo às Unidades de Informação (Nacional; Centrais; Regionais e Locais) tratamento³¹, a coordenação³² e a análise da informação (Luizio, 2009, p. 15).

Relativamente ao acesso à informação o sistema responde em função dos dados que o utilizador tem permissão para visualizar, considerando: o seu nível de segurança e unidade; as regras de visibilidade em função da matéria e competência territorial; o resultado da pesquisa é negativo, independentemente de existir informação relacionada no sistema, sempre que o utilizador não possua permissão para aceder aos dados (Luizio, 2009, p. 15).

Após inserção de dados, deve ser efetuado relatório de coordenação por utilizador com nível de segurança elevado. É a forma mais fiável de obter informação do SIIC. Tem subjacente um mecanismo de reciprocidade. "Quem alimenta o sistema, é informado daquilo que nele existe". O relatório de coordenação não possibilita o acesso direto à informação. Fornece dados sobre objetos em conflito e permite o contacto entre as partes e consequente coordenação das investigações. Os conflitos relacionados com AI de nível de segurança, obrigam ao contacto com a Unidade Nacional. (Luizio, 2009, p. 16).

³¹ O sistema informático deteta automaticamente coincidências relacionadas com: pessoas; pessoas coletivas; grupos organizados; locais; viaturas; embarcações/Aeronaves; armas; telefones; obras de arte; contas bancárias; cartões bancários; notas bancárias e títulos de crédito.

³² O Coordenador procede à classificação da AI quanto à natureza, nível de segurança, infração, tipo de coordenação, distribuição e movimentos.



Refira-se ainda que o sistema contém dados relativos a objetos transacionados, salvados, cadáveres/desaparecidos, permite o reconhecimento fotográfico e o reconhecimento de obras de arte (Luizio, 2009, p. 18).

O Sistema de Pesquisa *OnLine* possibilita o acesso a informação confirmada “não classificada”, informação administrativa, reconhecimentos fotográficos/obras arte, informação internacional INTERPOL/SCHENGEN, informação protocolada, identificação civil, Serviços Prisionais, PSP (armas/viaturas), registo automóvel, registo predial, registo de pessoas coletivas, identificação criminal e contumazes (Luizio, 2009, p. 18).

(2) GNR

O Sistema Integrado de Informações Policiais e Operacionais (SIIOP), que consiste num sistema informático centralizado e alargado a todo o dispositivo, permite o suporte à decisão/ação, baseado em informação alargada e em tempo real, bem como a uniformização de procedimentos em toda a hierarquia da GNR (Guedes, 2010, p. 30), tem por função constituir-se num repositório único que, comunicando com todos os outros sistemas, permitisse a integração de toda a informação possibilitando consultas "*just-in-time*"; Operações de pesquisas avançadas; Análises e operações de "*Business Intelligence*" que permitem transformar os "dados" em "informações policiais" com valor acrescentado; uniformizar "Processos de Negócio" globais; um adequado tratamento da informação estatística essencial à tomada de decisão operacional e estratégica. Este sistema tem a finalidade e inovar, simplificar, desmaterializar e tornar mais eficientes os "processos funcionais" em todas as áreas da atividade Operacional da GNR, garantindo uma racionalização da gestão, a adoção de uma administração eficaz e a efetiva materialização de redes de partilha e de interoperabilidade com outros organismos nacionais e internacionais (Guedes, 2010, p. 32).

O Sistema SIIOP disponibiliza ferramentas que permitem organizar e manter atualizada a Informação necessária ao exercício das missões da GNR, com o objetivo de estar disponível em todo o dispositivo, garantindo o registo, classificação e acesso à informação, mas preservando a necessidade de saber (Grenho, 2009, p. 21).

Está também previsto, um módulo do sistema SIIOP, que permite a georreferenciação dos objetos tipificados de maneira a que seja possível visualizar a informação tanto num formato alfanumérico como geográfico, bem como um módulo do sistema SIIOP, que permite uma análise visual, baseada nos produtos i2 que permite a correlação da informação de uma forma muito mais direta (Grenho, 2009, p. 21).



O sistema implementa a relação e enquadramento da informação afeta às duas áreas funcionais da GNR, isto é: Operações e IC de maneira a coadjuvar a Gestão Operacional de toda a Guarda.

O sistema pode incorporar um módulo de Análise (ainda não desenvolvido) que visa promover a agilização da recolha, armazenamento e análise de dados por fenómeno ou necessidade, permitindo interagir com os produtos (e.g. *Analyst Notebook*) (Grenho, 2009, p. 28). Permite ainda extrair relatórios estatísticos, cujos mapas serão incorporados no sistema ficando disponíveis para o utilizador autorizado.

Contudo, o SIIOP, que foi e é um projeto extremamente ambicioso, sofre de uma falha estrutural, ao nível da tecnologia dos processos, pois devido à grande dispersão do Dispositivo Territorial não tem sido viável estender a estrutura de rede a todos os Postos da GNR. Este constrangimento leva à atual impossibilidade de possuir num único repositório toda a informação operacional, com evidentes prejuízos para a atuação não apenas da GNR mas de todo o Sistema de Segurança Interna.

(3) PSP

A Lei Orgânica da PSP consagra duas estruturas de Informações com competências de informações, uma na dependência do Departamento de Informações Policiais (DIP) e outra adstrita ao Departamento de Investigação Criminal (DIC) (Vieira, 2013).

O SEI é o sistema de informação da PSP, detentor de dados que suportam a atividade operacional em diversas áreas como o trânsito, a IC, licenciamento e fiscalização. É um sistema informático bem mais abrangente onde, para além da informação típica de Polícia Judiciária, se inclui a informação de polícia administrativa e, ainda, todas as demais aplicações informáticas de gestão das várias áreas de atuação. Todas as áreas de atuação têm em comum um Repositório de Informação, o que permite a reutilização da informação e o seu enriquecimento (Bagina, 2009, p. 29)

As definições de segurança do SEI assentam no critério hierárquico e na atribuição de perfis a cada um dos elementos da PSP com base no posto que ocupam e nas funções que exercem (Bagina, 2009, p. 29).

Considerando apenas a segunda, que tem a seu cargo a vertente de apoio à estrutura de IC, podemos desde logo referir que constitui um pilar fundamental no trabalho diário das diversas Subunidades.

(4) SEF

O SEF gere e é responsável pelo Sistema Integrado de Informação SII no qual regista os dados pessoais que recolhe no exercício das suas atribuições legais de gestão do



controlo de entrada, permanência e saída de cidadãos estrangeiros, a prevenção de um perigo concreto ou a repressão penal relacionada com as suas atribuições O Sistema é constituído por dados pessoais e relativos a bens jurídicos, integrando dados de cidadãos controlados em trânsito nas fronteiras terrestres, marítimas e aéreas, bem como da sua permanência e atividades em território nacional; identificação e paradeiro de cidadãos estrangeiros ou nacionais de Estados membros da EU no que concerne a suspeita da prática ou a prática de auxílio à imigração ilegal, estada (alojamento em unidades hoteleiras e residência) de estrangeiros, bem como da sua permanência e atividades em território nacional (Pedro, 2009, p. 38).

Os dados podem ser comunicados no âmbito das convenções internacionais e comunitárias a que Portugal se encontra vinculado, bem como no âmbito da cooperação internacional ou nacional, às FFSS e a serviços públicos, no quadro das atribuições legais da entidade que os requer e apenas quanto aos dados pertinentes à finalidade para que são comunicados. Isto é, nos termos da lei, a comunicação depende de requerimento de uma força/serviço de segurança ou serviço público (Pedro, 2009, p. 39).

O SEF é ainda responsável pelo sistema de informação do passaporte eletrónico português (SIPEP), que se destina a registar, armazenar, tratar, manter atualizada, validar e disponibilizar a informação associada ao processo de concessão dos passaportes, designadamente, assinatura e dados biográficos e biométricos. Os dados constantes do SIPEP só podem ser comunicados aos órgãos de polícia criminal e autoridades judiciais, para efeitos de investigação ou de instrução criminal, dados registados no SIPEP em condições que respeitem o disposto no n.º 3 do artigo 4.º do Regulamento (CE) n.º 2252/2004, do Conselho, de 13 de Dezembro, e quando os dados não possam ou não devam ser obtidos das pessoas a que respeitem e as entidades em causa não tenham acesso à base de dados.

A comunicação depende de solicitação fundamentada de magistrado ou de autoridade policial e deve ser recusada quando o pedido não se apresentar devidamente fundamentado. Não é permitida qualquer forma de interconexão dos dados existentes no sistema de informação do passaporte eletrónico português, salvo nos termos previstos em legislação especial» (Pedro, 2009, p. 41).

Apêndice 4 – Ciclo de produção de Informações

Sumarizando os conceitos supra descritos as *Informações*, enquanto processo, traduzem-se num conjunto de ações em que certos tipos de informação são solicitados, pesquisados e compilados, analisados e disseminados, com o objetivo de gerar conhecimento necessário para a decisão.

“O **Ciclo de Produção de Informações** é uma sequência das atividades de informações na qual a notícia é obtida, transformada em informação e explorada” (Exército, 2009, pp. 3-1). Este processo, visa espelhar um processamento cíclico incorporando um determinado conjunto de etapas, repetidas e interdependentes, com a fim de adicionar valor às premissas iniciais de gerando um produto consistentemente melhorado e adaptado aos requisitos estabelecidos pelos decisores ou requerentes.

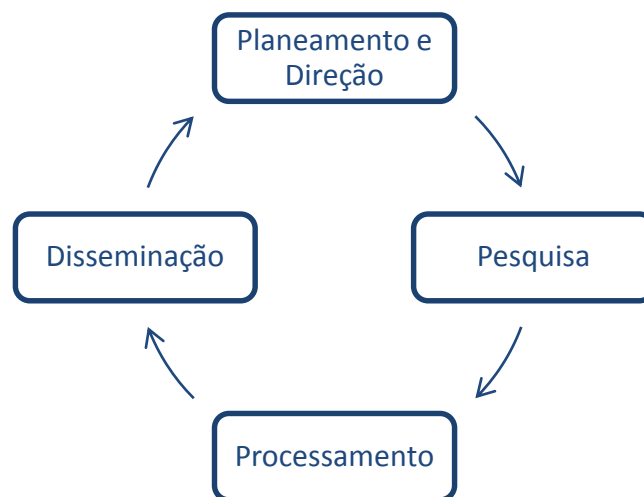


Fig.4 – Diagrama do Ciclo de Produção de *Informações*.

Fonte: (GNR, 2012b, p. 7)

A primeira fase, **Direção e Planeamento**, dá início ao processo com a definição das necessidades de informação pelo “cliente” (entidade que necessita da informação), seguindo-se o planeamento das ações necessárias à satisfação dos requisitos decorrentes dessa necessidade, coordenando todos os meios disponíveis (GNR, 2012b, p. 9). Os pedidos são dissecados em informação requerida e são estabelecidas prioridades, procurando-se perceber os dados a coligir para estimar ou inferir as respostas solicitadas. As necessidades de dados são usadas como base para o estabelecimento de planos de pesquisa com elementos acerca dos dados a ser recolhidos e dos «alvos», sobre os quais os dados podem ser obtidos (Waltz, 2003, cit. por Menezes, 2012, p. 21). O planeamento e direção são também responsáveis pelo final do ciclo, uma vez que as



informações difundidas, que suportam o processo de decisão, são geradoras de novos requisitos (FBI, 2004).

A segunda fase, que consiste na pesquisa, resulta da primeira (sendo essencial uma orientação precisa e coordenação centralizada) e tem por objeto primeiro a obtenção dos dados que sustentam o processo. Para o efeito, seguindo o plano, previamente estabelecido, é atribuído a fontes humanas ou técnicas o trabalho de recolha dos dados necessários aos requisitos (Waltz, 2003, cit. por Menezes, 2012, p. 21), sendo levadas a cabo, pelos órgãos de pesquisa, atividades como entrevistas, vigilâncias, ligação e solicitação de informação a outras entidades (FBI, 2004), recorrendo-se também à pesquisa de fontes abertas (OSINT). Nesta fase é essencial garantir a proteção das fontes³³, para além de ser fundamental averiguar a sua credibilidade³⁴, capacidade técnica³⁵, bem como o grau de verosimilhança³⁶ dos dados ou notícias obtidos (GNR, 2012b, p. 14).

A terceira etapa do ciclo compreende o **processamento** dos dados recolhidos e a sua exploração, passando pela conversão para formatos que permitam o tratamento pelos analistas, podendo incluir ações como a tradução, descriptação, e organização em bases-de-dados de informação, essenciais ao processo de análise (FBI, 2004). Esta fase permite verificar se os requisitos estabelecidos no plano de pesquisa estão em consonância com o desejado, podendo ser redefinidos, caso os dados recebidos não sejam satisfatórios (Waltz, 2003, cit. por Menezes, 2012, p. 22). No processamento podemos estabelecer cinco subfases, nomeadamente: registo³⁷; avaliação³⁸; análise; integração³⁹ e interpretação (GNR, 2012b, p. 14).

A análise consiste em determinar e isolar os elementos significativos das notícias e informações, para subsequente interpretação, “dissecando” os dados e individualizando os elementos importantes e integrando-os, entre si e com outras notícias ou informações, através de dedução lógica (FBI, 2004), aplicando métodos das ciências sociais, métodos

³³ Fontes são as diversas pessoas, objetos, atividades ou entidades diversas, das quais se podem obter dados ou notícias.

³⁴ Grau de confiança que merece a fonte ou origem.

³⁵ Grau de conhecimento que a fonte possui de um assunto, sendo particularmente relevante em assuntos técnicos ou especializados.

³⁶ Probabilidade dos dados ou notícias serem ou não verdadeiros.

³⁷ Tem por finalidade ordenar, sistematizar e categorizar as notícias por forma a facilitar o seu estudo e permitir o estabelecimento de relações entre dados aparentemente não relacionados.

³⁸ Tem por finalidade determinar o valor da notícia atendendo à sua pertinência, oportunidade, confiança e exatidão (GNR, 2012b, p. 17).

³⁹ Consiste na combinação dos elementos individualizados, obtidos por análise, a fim de se formularem uma ou mais hipóteses lógicas (GNR, 2012b, p. 18).



analíticos e técnicas estatísticas (PJ, 2010, p. 6), por forma a produzir informações que respondam aos requisitos estabelecidos.

A última fase do ciclo é a **difusão**, onde deverá ser garantido que as informações necessárias chegam às entidades (“clientes” que delas necessitam), em tempo oportuno e numa forma apropriada, pelos meios adequados (GNR, 2012b, p. 18). As respostas às questões colocadas são elaboradas em vários formatos, que podem variar consoante o solicitado, podendo ir desde imagens dinâmicas de sistemas, diagramas de ligação, até aos relatórios formais, entre outros (Waltz, 2003, cit. por Menezes, 2012, p. 22). A difusão deverá ter em consideração os princípios de clareza (diferenciar entre fatos e interpretação), concisão, normalização (sequência lógica e formatos normalizados), urgência (respeitando a oportunidade e necessidade, ainda que com sacrifício do processamento), necessidade de conhecer (apenas a quem necessita da informação), revisão contínua (atualização permanente), segurança (adequar a classificação a atribuir) e proteção da fonte (apesar de em alguns casos, nomeadamente no âmbito processual criminal, esta premissa colidir com a legalidade e, por esse motivo, não poder ser respeitada na íntegra).



Apêndice 5