INSTITUTO UNIVERSITÁRIO MILITAR

DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

CURSO DE ESTADO-MAIOR CONJUNTO

2021/2022

TII

O IMPACTO DA TECNOLOGIA NO POLICIAMENTO

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IUM, SENDO DA RESPONSABILIDADE DA SUA AUTORA, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DAS FORÇAS ARMADAS PORTUGUESAS OU DA GUARDA NACIONAL REPUBLICANA.

Sara Isabel dos Santos Quinta Albuquerque

MAJ GNR INF

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O IMPACTO DA TECNOLOGIA NO POLICIAMENTO

MAJ GNR INF Sara Isabel dos Santos Quinta Albuquerque

Trabalho de Investigação Individual do CEMC

Pedrouços 2022

INSTITUTO UNIVERSITÁRIO MILITAR
DEPARTAMENTO DE ESTUDOS PÓS-GRADUADOS

O IMPACTO DA TECNOLOGIA NO POLICIAMENTO

MAJ GNR INF Sara Isabel dos Santos Quinta Albuquerque

Trabalho de Investigação Individual do CEMC

Orientadora: TCOR GNR INF Cláudia Margarida dos Santos

Coorientadora: MAJ GNR INF Lídia de Jesus Janeiro Magalhães

Pedrouços 2022

Declaração de compromisso Antiplágio

Eu, **Sara Isabel dos Santos Quinta Albuquerque**, declaro, por minha honra, que o documento intitulado "**O impacto da tecnologia no policiamento"** corresponde ao resultado da investigação por mim desenvolvida, enquanto auditora do **Curso de Estado-Maior Conjunto 2021/2022**, no Instituto Universitário Militar, e que é um trabalho original, em que todos os contributos estão corretamente identificados em citações e nas respetivas referências bibliográficas.

Tenho consciência que a utilização de elementos alheios não identificados constitui grave falta ética, moral, legal e disciplinar.

Pedrouços, **04** de **maio** de **2022**

Sara Isabel dos Santos Quinta Albuquerque

Assinado por: **SARA ISABEL DOS SANTOS QUINTA ALBUQUERQUE**
Num. de Identificação: 12411279
Data: 2022.06.29 18:09:10+01'00'

CARTÃO DE CIDADÃO

Agradecimentos

Dirijo os meus sinceros agradecimentos à Tenente-coronel Cláudia Santos, por ter aceite orientar o trabalho e por todos os ensinamentos que, com amizade, partilhou comigo, de forma incansável, os quais foram essenciais ao desenvolvimento da investigação e à obtenção dos resultados.

Da mesma forma, agradeço à Major Lídia Magalhães, coorientadora, pelo permanente acompanhamento, dedicação e amizade, assim como sentido crítico, que muita importância tiveram, também, no desenvolvimento do trabalho.

Agradeço, ainda, a todos os que contribuíram para a realização da investigação, em especial as entidades entrevistadas, cuja experiência e conhecimento foram essenciais à análise e ao alcance dos objetivos propostos, destacando, em particular, o Major Gonçalo Serrão, pela partilha, sentido crítico e pertinentes sugestões sobre a temática em estudo.

Dedico, ainda, uma palavra de apreço ao Senhor Comandante Luís Carona Jimenez, Diretor do Curso de Estado-Maior Conjunto, assim como aos camaradas auditores deste curso, companheiros nesta jornada.

Por fim, agradeço de coração à minha família, ao meu marido Tiago, aos meus filhos Tiago e Francisco, e à minha mãe Isabel, pela compreensão, apoio e amor incondicionais, imprescindíveis para conseguir cumprir este desafio, mas, especialmente, pelas horas em que estive ausente.

O meu muito obrigada.

Índice

Índice de Apêndices

Índice de Figuras

Índice de Quadros

Resumo

O desenvolvimento tecnológico é reconhecido como uma mais-valia para a eficácia e eficiência do serviço prestado pelas forças de segurança.

Neste domínio, apesar de a Inteligência Artificial assumir um papel preponderante, a sua implementação aporta questões relacionadas com a salvaguarda de direitos fundamentais, nomeadamente a proteção de dados, as quais têm que ser dirimidas para a utilização desta tecnologia.

Na senda, o objetivo desta investigação foi propor boas práticas para a aplicação desta tecnologia nos sistemas de videovigilância da Guarda Nacional Republicana em espaços públicos, cumprindo o ordenamento jurídico vigente.

Para tal intento, recorreu-se a uma estratégia de investigação qualitativa e a um desenho de pesquisa por estudo de caso, sustentado em pesquisa bibliográfica e análise documental, assim como na recolha de dados e informações através da realização de entrevistas semiestruturadas, que aportaram valor acrescentado e permitiram uma análise comparada, numa perspetiva de *benchmarking*, no caso em apreço, à situação da Guarda Nacional Republicana.

Foi possível concluir sobre a importância da aplicabilidade de Inteligência Artificial nos sistemas de videovigilância policial em espaços públicos, assim como propor boas práticas passíveis de implementação pela Instituição, sustentadas pelas experiências das forças congéneres europeias e pelos níveis político, técnico e institucional no cômputo nacional.

Palavras-chave:

Policiamento, Inteligência Artificial, Videovigilância Policial, Tecnologia.

Abstract

Technological development is recognized as an asset to the effectiveness and efficiency of the service provided by the security forces.

In this domain, although Artificial Intelligence assumes a leading role, its implementation raises issues related to the safeguarding of fundamental rights, namely data protection, which have to be solved for the implementation of this technology.

On the way, the objective of this investigation was to propose good practices for the application of this technology in the video surveillance systems of the Guarda Nacional Republicana in public spaces, complying with the current legal system.

For this purpose, we used a qualitative research strategy and a case study research design, based on bibliographic research and document analysis, as well as on the collection of data and information through semi-structured interviews, which added value added and allowed a comparative analysis, from a benchmarking perspective, in the present case, to the situation of the Guarda Nacional Republicana.

It was possible to conclude on the importance of the applicability of Artificial Intelligence in police video surveillance systems in public spaces, as well as to propose good practices that can be implemented by the Institution, supported by the experiences of European counterparts and by the national political, technical and institutional levels.

Keywords:

Policing, Artificial Intelligence, Police Surveillance, Technology.

Lista de abreviaturas, siglas e acrónimos

A

Art.º	Artigo
AC	*Arma dei Carabinieri*

C

CE	Comissão Europeia
CRP	Constituição da República Portuguesa
CNPD	Comissão Nacional de Proteção de Dados
CEPD	Comité Europeu para a Proteção de Dados

D

DLG	Direitos, liberdades e garantias

F

FS	Forças de Segurança

G

GC	*Guardia Civil*
GN	*Gendarmerie Nationale*
GNR	Guarda Nacional Republicana

I

IA	Inteligência Artificial
IUM	Instituto Universitário Militar

M

MH	*Marechaussee* Holandesa

N

NATO	*North Atlantic Treaty Organization*
N.º	Número

O

OSCE	Organização para a Segurança e Cooperação na Europa
OE	Objetivo Específico
OG	Objetivo Geral

P

PE	Parlamento Europeu

Q

QC	Questão central

QD	Questão derivada
R	
RASI	Relatório Anual de Segurança Interna
RGPD	Regime Geral de Proteção de Dados
S	
SGMAI	Secretaria Geral do Ministério da Administração Interna
T	
TII	Trabalho de Investigação Individual
U	
UE	União Europeia

1. Introdução

O presente trabalho é subordinado ao tema "O impacto da tecnologia no policiamento".

O desenvolvimento tecnológico é, reconhecidamente, uma mais-valia no que se refere ao incremento da eficácia e da eficiência das Forças de Segurança (FS), no quadro da sua atuação, e, também, nas ferramentas que pode oferecer, que potenciam a qualidade do serviço prestado.

Neste domínio, a Inteligência Artificial (IA) tem assumido um papel preponderante, apesar de a sua implementação, indubitavelmente necessária, aportar questões relacionadas com a salvaguarda de direitos fundamentais dos cidadãos, nomeadamente a proteção de dados pessoais, as quais têm que ser dirimidas para se poder aplicar esta tecnologia, em conformidade com os parâmetros de segurança e fiabilidade.

A crescente complexidade dos desafios securitários e a necessidade de aumentar a eficácia operacional, têm levado as FS a implementar diversas ferramentas tecnológicas, no desiderato de manter a segurança e a tranquilidade públicas. Neste particular, têm assumido especial relevância os sistemas de videovigilância policial em espaços públicos, cujas mais-valias são reconhecidas para a salvaguarda de pessoas e bens, em especial nas zonas onde existe criminalidade grave.

A evolução destes sistemas permite conjugar a recolha de imagens e a capacidade de análise destas, constituindo-se a IA, nesse domínio, um instrumento muito relevante, suscetível de potenciar a atuação das FS, especialmente por incrementar a capacidade preditiva e a capacidade de investigação, através do processamento e análise de grandes volumes de informação e da correlação de situações que poderão permitir antecipar eventos e alocar meios policiais de uma forma mais eficaz e oportuna.

Não obstante o interesse e as mais-valias sobre a utilização destes meios tecnológicos, a sua implementação requer, obrigatoriamente, a garantia de que os sistemas são seguros e fiáveis, no que se refere à salvaguarda dos direitos, liberdades e garantias (DLG) dos cidadãos, sobretudo o da privacidade, implicando, para corresponder aos mais elevados padrões de conformidade, o estabelecimento e a obediência a critérios rigorosos de utilização, assim como o desenvolvimento de medidas que minimizem os riscos e promovam a proteção de dados pessoais.

Efetivamente, o desenvolvimento de IA tem aumentado exponencialmente ao longos dos últimos anos, fazendo já parte do quotidiano da sociedade, que reconhece os benefícios

da sua utilização, mas, também, os riscos associados. Os resultados desta utilização, positivos ou negativos, dependerão do uso que for feito desta tecnologia, na medida em que tanto pode facilitar atividades criminosas e potenciar as ameaças inerentes, ou, ao contrário, poderá oferecer importantes vantagens e benefícios, inclusive, para fazer face a tais ameaças, reduzindo os riscos através de sistemas mais seguros (através de IA).

Desta forma, revela-se de extrema importância determinar os limites e os critérios para o desenvolvimento e utilização da tecnologia com IA, no sentido de se conseguir compatibilizá-la com os direitos fundamentais dos cidadãos e com a vida em sociedade, maximizando os seus benefícios e reduzindo os riscos que possam estar associados.

Uma outra questão que se torna pertinente é o grau de autonomia dos sistemas com aplicação de IA, assim como a intervenção humana, no que se refere à validação e decisão sobre ações que tenham impacto sobre os cidadãos, sobretudo no que respeita aos seus DLG.

Neste enquadramento, a União Europeia (UE) tem o objetivo de regular tanto o desenvolvimento como a utilização desta tecnologia, no seio dos Estados-Membros, através da definição de opções políticas que concorram para um desenvolvimento fiável e seguro, na Europa, e que possibilitem a implementação de um ordenamento jurídico que salvaguarde os direitos fundamentais dos cidadãos.

Torna-se, assim, preponderante estudar a aplicação de IA nos sistemas de videovigilância policial em espaços públicos, em cumprimento do ordenamento jurídico em vigor, aferindo boas práticas que possibilitem a implementação pela Guarda Nacional Republicana (GNR).

Em tal contexto, o trabalho tem como objeto de estudo a IA na videovigilância policial, delimitando-se a investigação, no domínio temporal, ao período compreendido desde 2005 (ano que corresponde à vigência dos primeiros normativos jurídicos reguladores da proteção de dados) até à atualidade; no domínio espacial, à zona de ação da GNR em Portugal; e, em conteúdo, à aplicação de IA nos sistemas de videovigilância policial implementados pela GNR em espaços públicos, analisando-se as perspetivas de FS congéneres europeias, concretamente a *Guardia Civil* (GC) Espanhola, a *Gendarmerie Nationale* (GN) Francesa, a *Arma dei Carabinieri* (AC) Italiana e a *Marechaussee* Holandesa (MH), à luz da regulamentação europeia e dos respetivos procedimentos internos, numa ótica de *benchmarking*, assim como os níveis político e técnico, no cômputo nacional, no que se refere à autorização para implementação e utilização destes sistemas e aos requisitos técnicos e medidas de segurança que devem ser implementadas.

O Objetivo Geral (OG) desta investigação é propor boas práticas para a aplicação de IA nos sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor.

Para tal desiderato, foram definidos três Objetivos Específicos (OE):

OE1. Analisar o ordenamento jurídico aplicável à videovigilância policial em espaços públicos, no contexto europeu e a sua transposição nacional.

OE2. Analisar a aplicação de IA nos sistemas de videovigilância da GNR em espaços públicos, à luz do ordenamento jurídico em vigor.

OE3. Analisar a aplicação de IA nos sistemas de videovigilância em espaços públicos pelas FS congéneres europeias, à luz do ordenamento jurídico em vigor.

Dos referidos OG e OE decorrem as seguintes Questões Derivadas (QD):

QD1. Qual o ordenamento jurídico aplicável à videovigilância policial, no contexto europeu, e qual a sua transposição nacional?

QD2. Pode a GNR aplicar IA nos sistemas de videovigilância em espaços públicos, em cumprimento do ordenamento jurídico em vigor?

QD3. Aplicam as FS congéneres europeias IA nos seus sistemas de videovigilância em espaços públicos, em cumprimento do ordenamento jurídico em vigor?

Na senda, a Questão Central (QC) da investigação é a seguinte: que boas práticas podem ser adotadas para aplicar IA em sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor?

No que se refere à organização do trabalho, no primeiro capítulo é feita a introdução da problemática e dos objetivos da investigação; no segundo capítulo é estabelecido o enquadramento concetual e metodológico; no terceiro capítulo é apresentado o ordenamento jurídico aplicável à videovigilância policial, no contexto europeu e a sua transposição nacional; no quarto capítulo é analisada a aplicação de IA nos sistemas de videovigilância policial, abordando a análise à luz do ordenamento jurídico, a sua implementação, incluindo os níveis político, institucional e técnico, e a perspetiva de FS congéneres europeias; no quinto capítulo é feita a discussão de resultados, com a apresentação de propostas de boas práticas, neste domínio; e, no sexto e último capítulo, são apresentadas as conclusões, com indicação das limitações à investigação e sugestão de estudos futuros e recomendações.

2. Enquadramento teórico, concetual e metodológico

O percurso de investigação iniciou-se com a definição do Estado da Arte, através de revisão literária de obras de referência e de investigações nesta área e da realização de entrevistas exploratórias a especialistas na temática.

No seguimento, estabeleceu-se a base concetual relevante para o objeto de estudo.

2.1 Enquadramento teórico e concetual

2.1.1 Revisão da literatura

A necessidade de detetar e identificar potenciais terroristas passou a ser um desígnio operacional, constituindo a recolha de dados, incluindo o tratamento e análise, requisitos essenciais ao combate ao crime, através do uso de meios automatizados associados à utilização de bases de dados, que colocam na ordem do dia a salvaguarda da privacidade e os limites entre segurança e liberdade (Lourenço e Costa, 2018, p. 58).

Na senda, Lourenço e Costa, salientam a preponderância das tecnologias no domínio da Segurança, sobretudo no que respeita à ocultação dos terroristas entre a população e o recurso destes ao anonimato, como vantagem às suas atividades criminosas, fator que confere às questões da identidade uma importância sem precedentes (2018, p. 58).

Nos últimos anos, as FS têm implementado ferramentas tecnológicas para obter melhores resultados e incrementar a eficiência operacional, especialmente em contexto de limitação de recursos e de escrutínio público, assim como de enquadramento legal mais restritivo sobre a atuação policial (Strom, 2017). Neste campo, subsiste, ainda, muito por apurar sobre a prevalência e a utilidade da tecnologia, à luz do enquadramento jurídico e sobre os fatores que influenciam a sua seleção e implementação (Strom, 2017).

Torna-se necessário construir uma base de conhecimento para justificar a implementação de nova tecnologia, pelas FS, centrada na forma como é utilizada e se melhora significativamente o policiamento, tanto internamente como para a comunidade (Strom, 2017).

De acordo com a Organização para a Segurança e Cooperação na Europa (OSCE), dois dos maiores desafios que as FS enfrentam são os fenómenos criminais cada vez mais complexos e transnacionais e uma sociedade cada vez mais exigente (2017).

Acompanhando a evolução dos fenómenos sociais e criminais, as FS tendem a implementar novas tecnologias, sobressaindo os sistemas de videovigilância em locais públicos (Pereira, 2017).

Verifica-se a implementação de sistemas de videovigilância em espaços públicos, decorrente, conforme Valente, da exigibilidade destes meios e da sua indispensabilidade para a salvaguarda dos bens jurídicos superiores, da segurança e ordem públicas, onde se impõe a verificação da existência de riscos objetivos (2014, p. 590).

A evolução dos sistemas de videovigilância vem conjugando a recolha de imagens com a capacidade de as analisar e criar um tipo de ação ou alerta, com base no resultado, exponenciando as operações de segurança (Security Magazine, 2021).

Neste contexto, a aplicação da IA constitui-se um instrumento poderoso na luta contra a criminalidade, exponenciando as capacidades de investigação, através da análise de grandes volumes de informação e da possibilidade de identificação de padrões; não obstante, a sua utilização requer os mais elevados padrões de conformidade com os DLG, assegurando, simultaneamente, uma proteção eficaz dos cidadãos, com o controlo humano subjacente, em especial, nas decisões que afetem as pessoas (UE, 2020).

A utilização do *big data* para processar dados pessoais, pelas FS, é já uma realidade, designadamente a utilização de algoritmos para identificar pessoas, através de dados biométricos e registo de imagens, da voz, do ADN ou de outros padrões, no quadro do combate ao terrorismo e criminalidade organizada (Lourenço e Costa, 2018).

Neste domínio, o Parlamento Europeu (PE) considera que o recurso à IA em sistemas de videovigilância, pelas FS, deve salvaguardar a privacidade dos cidadãos, denotando-se uma especial preocupação sobre a utilização de dados biométricos (SapoTek, 2021).

Crê-se, assim, pertinente estudar a aplicação de IA nos sistemas de videovigilância policial, pelo valor acrescentado que poderá aportar à função policial e, também, pela sensibilidade inerente à sua utilização, que requer a implementação das melhores práticas, em cumprimento do ordenamento jurídico em vigor, almejando minimizar o risco para os DLG dos cidadãos.

Nesta medida, considera-se relevante apurar boas práticas transponíveis para a GNR, com base na perspetiva de FS congéneres, na dimensão europeia (porquanto se regem pelos mesmos normativos jurídicos comunitários), assim como na análise dos pressupostos e requisitos que devam ser salvaguardados ao nível dos sistemas e dos seus operadores, no sentido de reunir um contributo para os procedimentos internos, como forma de tornar o modelo de policiamento mais eficaz e fiável para o cidadão.

Do que foi possível verificar, não foi, ainda, realizada nenhuma investigação com o objetivo de implementar IA em sistemas de videovigilância policial, o que aporta um grau de complexidade superior à presente investigação.

2.1.2 **Conceitos gerais**

O conceito de *Segurança*, de acordo com Bacelar Gouveia, pode encerrar múltiplos significados, embora do mesmo se possa deduzir um sentido mínimo comum, a proteção (2018, p.89). Para o presente trabalho, adota-se a definição de Bacelar Gouveia, que a refere como meio de ação, por um lado, convocadora de instrumentos, comportamentos e instituições, e, por outro, como atividade que tem por fim alcançar o resultado de se estar seguro, diminuindo ou eliminando os riscos que impeçam essa pretensão (2018, p.89).

Tal é reforçado por Fernandes que entende a Segurança como um desígnio que visa reduzir o risco ao máximo, apesar de admitir ser difícil proteger todas as vulnerabilidades, de forma absoluta (2020, p. 6).

Decorre do texto constitucional, Lei nº 1/1976, de 10 de abril, que todos os cidadãos têm direito à liberdade e à segurança, constituindo a garantia dos direitos e liberdades fundamentais uma das tarefas fundamentais do Estado.

É, assim, por via do texto constitucional e pela Lei de Segurança Interna, que o Estado prossegue, através das Polícias, a atividade de Segurança, necessidade coletiva que pode ser considerada um bem jurídico supra-individual, porquanto a todos beneficia, assim como interesse público "inato a uma comunidade democraticamente organizada, e por representar a face da cedência dos cidadãos ao poder político de uma das tarefas em troca de uma limitação estreita da liberdade*"* (Valente, 2014, p. 113).

Para o presente trabalho, adota-se, também, o conceito de *Policiamento*, como a atividade prosseguida pela Polícia, que "em sentido material consiste no modo de atuação […] destinado a prevenir os perigos que ameaçam determinados bens jurídicos […] da Constituição, a legalidade democrática, a segurança interna e os direitos dos cidadãos" (Raposo, 2013, pp. 282-283).

Moleirinho, no contexto do policiamento preditivo, acrescenta, ainda, que a prevenção requer proatividade de atuação policial, exigindo análises preditivas que, por seu turno, requerem a identificação de padrões, por forma a antecipar e mitigar os riscos, informando a ação do decisor (2018, p.116).

Poderão ser encontradas diversas definições para o conceito de *Videovigilância*, sendo que se adota, para este trabalho, a constante no *Dossier* Temático da Secretaria Geral do

Ministério da Administração Interna (SGMAI), que a indica como "a observação feita com recurso a sistemas de vídeo (câmaras de filmar, sistemas de deteção automática de movimento, etc.)" (SGMAI, 2020, p. 4).

Caetano refere ser o propósito da vigilância habilitar as autoridades de polícia com informação que possibilite prevenir perturbações e adotar as providências necessárias para as evitar ou para identificar os autores (2008, p. 1166).

A este respeito, Bacelar Gouveia salienta a utilidade dos sistemas de videovigilância para fins preventivos, mas, também, para a investigação criminal, no pressuposto de cumprimento dos normativos legais (2018, p. 583).

Neste domínio, Moleirinho refere que os "modelos de policiamento mais preventivos têm vindo a utilizar capacidades proporcionadas pelo acesso a grandes volumes de dados, o designado *big data*, e também da analítica fundamentada na IA" (2021, p.5).

Neste seguimento, adota-se a definição de *Inteligência Artificial* do PE, que a refere como a capacidade de uma máquina reproduzir competências semelhantes às humanas, designadamente o raciocínio, a aprendizagem, o planeamento e a criatividade (PE, 2020).

É, neste contexto, estabelecido que a IA permite que os sistemas façam uma leitura do ambiente envolvente e resolvam problemas, para alcançar objetivos específicos, mediante dados já preparados ou recolhidos pelo próprio sistema, processando-os e respondendo, sendo capazes de adaptar o comportamento, até determinado ponto, por meio da análise e de forma autónoma (PE, 2020).

De acordo com Kai-Fu Lee, decorre a designada revolução total da IA, num ciclo de quatro vagas (IA da Internet, IA empresarial, IA com perceção e IA autónoma), em que a última terá um impacto profundo, representando a integração e o auge das precedentes, conjugando a capacidade de otimização com os poderes sensoriais, tendo como resultado que as máquinas não só compreendem o meio envolvente como lhe dão forma (2018, p. 131).

Outra importante distinção reside em estabelecer se o sistema é verdadeiramente *autónomo* ou simplesmente *automatizado*, isto é, se executa tarefas segundo regras definidas (com baixa autonomia, sendo descrito como automatizado) ou se goza de controlo sobre a forma de execução, tendo determinado grau de autonomia (descrito como totalmente autónomo) (Morgan et al., 2020, p. 9).

Salienta-se o desenvolvimento de sistemas mais sofisticados, capazes de aprendizagem automática, e de, progressivamente, melhorar o desempenho através do

reconhecimento de padrões em grandes volumes de dados e da introdução de ações corretivas para potenciar a capacidade de classificar futuros padrões, sem programação para tal, assim como de outra classe de sistemas de aprendizagem automática, ainda mais sofisticada, com capacidade de aprendizagem profunda, baseada em redes neurais profundas, que habilitaram avanços significativos em sistemas de visão computacional e reconhecimento de imagem. Levantam-se, assim, questões relacionadas com o controlo e supervisão destes sistemas e a responsabilidade sobre as consequências, constituindo o grau de envolvimento humano o fator basilar (Morgan et al., 2020, pp. 10-11).

2.2 Metodologia

A investigação seguiu as normas em vigor no Instituto Universitário Militar (IUM), tendo-se dado primazia à utilização de fontes primárias.

Considerando o objeto de estudo, o investigador adotou a posição ontológica do Construtivismo, atendendo a que os fenómenos sociais são produzidos pelas interações entre os atores sociais e entre estes e a sua envolvente, os quais se encontram em constante mutação (Bryman, 2012). Esta posição sustentou na necessidade de adaptação da GNR face à evolução da sociedade e dos diversos atores e fenómenos, designadamente os de natureza social e criminal.

Relativamente ao posicionamento epistemológico, assumiu-se o Interpretativismo, no pressuposto de que a realidade molda o ator e é, simultaneamente, moldada por este, considerando-se ser a posição que melhor permitiria compreender o objeto de estudo (Santos & Lima, 2019). Esta opção consubstancia as medidas e procedimentos implementados pela Instituição, decorrente da necessária adaptação à evolução da sociedade e dos diversos atores e fenómenos, que influenciam o ambiente social onde são desenvolvidas as funções policiais e a esfera do cidadão que, por sua vez, também é preponderante neste processo.

Optou-se pelo raciocínio dedutivo, partindo de premissas gerais para uma realidade particular (Freixo, 2012, p.19), com base no conhecimento reunido de conclusões provenientes de premissas gerais, para aplicar numa realidade particular da GNR, tendo em vista a implementação, de forma transversal, e em benefício dos procedimentos internos da Instituição.

A investigação seguiu uma estratégia qualitativa, baseada em pesquisa bibliográfica e análise documental, assim como na recolha de dados e informações através da realização de entrevistas semiestruturadas, conjugando valores conhecidos e articulados postulados com o conhecimento e a experiência proveniente das entrevistas pessoais, que aportam valor

acrescentado e permitem uma análise comparada, numa perspetiva de *benchmarking*, no caso em apreço, à situação da GNR.

O desenho de pesquisa foi o estudo de caso, atendendo a que se procurou recolher informação detalhada sobre uma unidade de estudo, inserindo-se nas estratégias qualitativas e com um caráter analítico (Santos & Lima, 2019).

O objeto de estudo é a IA na videovigilância policial e a investigação delimitou-se em três domínios: temporal, espacial e de conteúdo (Santos & Lima, 2019).

No domínio temporal, delimitou-se ao período compreendido desde 2005, ano que corresponde aos primeiros normativos jurídicos reguladores da proteção de dados, até à atualidade. Espacialmente, à análise nacional, da GNR, e, em conteúdo, à aplicação de IA na videovigilância policial da GNR, aferindo-se as perspetivas das congéneres, GC, GN, AC e MH, à luz da regulamentação europeia e respetivos procedimentos internos, numa ótica de benchmarking, e conjugando, ainda, com a análise dos níveis político, técnico e institucional, no cômputo nacional.

A identificação do problema de investigação é fundamental para a definição do percurso, pois dele decorre a formulação da QC e respetivas QD, elementos chave do processo científico (Santos & Lima, 2019). Assim, a QC que norteia a investigação, é: que boas práticas podem ser adotadas para aplicar IA em sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor?

2.2.1 Percurso metodológico

Numa primeira fase, enquadrou-se o tema e definiu-se o corpo de conceitos, identificando as fontes primárias e secundárias de informação a pesquisar, e estabeleceu-se o *Estado da Arte*. Procedeu-se à revisão da literatura e à realização de entrevistas exploratórias, o que permitiu definir o objeto de investigação e respetivos objetivos, geral e específicos, bem como formular o problema e desenhar o modelo de análise (Apêndice A), utilizado ao longo da investigação, que permitiu alcançar com rigor as conclusões da investigação e selecionar o procedimento metodológico de investigação mais adequado.

Na segunda fase, aplicou-se o modelo de análise, à luz dos conceitos estabelecidos e em conjugação com os instrumentos de pesquisa e de recolha de dados que se indicam:

- Análise documental, baseada na recolha e na análise de fontes documentais (Bryman, 2012, p. 543);

– Entrevistas, semiestruturadas, para obtenção de dados que não são possíveis a partir de fontes documentais e que são relevantes para a investigação (Freixo, 2012, p. 220).

2.2.2 Método

A análise documental incidiu, essencialmente, em fontes primárias, de entre as quais obras de referência, legislação europeia e nacional, documentos oficiais e publicações doutrinárias das Instituições.

As entrevistas visaram, por um lado, complementar a análise documental, trazendo conhecimento acrescentado, pela experiência e tecnicidade que os entrevistados reúnem, e, por outro, obter informação específica, que não seria possível de outra forma. Atendendo às Entidades visadas e às circunstâncias relacionadas com a situação pandémica, todas as entrevistas foram respondidas por e-mail, tendo as internacionais sido redigidas em língua inglesa e, subsequentemente, traduzidas. O conteúdo das respostas das FS foi alvo de análise com base na recolha e identificação dos elementos-chave, convertidos em segmentos, por forma a habilitar a conversão quantitativa das respostas, com base no número de vezes em que são repetidos (os segmentos ou as ideias subjacentes), no contexto da entrevista aplicada (Sarmento, 2013, pp. 53-54) – respostas transcritas em Apêndices D, E e F.

A seleção de pessoas entrevistadas foi deixada ao critério de cada FS, considerando a especificidade do objeto de estudo, tendo sido selecionados Oficiais com funções e experiências relevantes para o estudo em apreço.

A definição das entidades a entrevistar, contemplou três níveis e seguiu os seguintes critérios:

1. Nível político - MAI | entidade que aprova os projetos de videovigilância policial e regulamenta os requisitos decorrentes dos normativos jurídicos; e CNPD | autoridade nacional de controlo e supervisão (não concedeu entrevista);
2. Nível institucional - FS | análise da implementação pela GNR e pelas FS congéneres;
3. Nível técnico - Motorola *Solutions* – *Avigilon* | empresa que assegura o fornecimento, instalação, manutenção e substituição dos equipamentos de videovigilância às FS (com vista a complementar a investigação, aportando-lhe a perspetiva dos requisitos técnicos).

Foi aplicado um guião estabelecido *à priori*, mas possibilitando apresentar dados abertamente (Quivy & Campenhoudt, 2013, pp. 192-193), aos entrevistados em Quadro 1:

Quadro 1 – Relação de entrevistados

NÍVEL	ENTIDADE/FUNÇÃO | ENTREVISTADO		DIMENSÕES
Institucional	Guardia Civil | Chefe da Unidade de IT – UTPJ Major Miguel Fayos Mestre	E1	- Policiamento Preditivo -Videovigilância Policial - Analítica de Vídeo - RGPD
	Gendarmerie Nationale | Coordenador de IA e Administrador de Dados General Perrot	E2	
	Marechaussee | Assessora e Perita em Dados Capitão Mariel van Staveren	E3	
	Arma dei Carabinieri | Gabinete de Cooperação Internacional Coronel Antonio Servedio	E4	
	GNR | Chefe da Repartição de Operações/Comando Operacional Major Gonçalo Serrão	E5	
Político	MAI | Secretário de Estado Adjunto e da Administração Interna (SEAAI) Antero Luís	E6	-Videovigilância Policial - Analítica de Vídeo - RGPD
Técnico	Motorola Solutions | Avigilon - Video Security & Access Control Gonçalo Pereira Pessoa	E7	-Videovigilância Policial - Analítica de Vídeo - RGPD

Com a investigação, procurou-se reunir um contributo sólido, útil e passível de ser adotado na Instituição, com base num estudo credível e sustentado numa abordagem inovadora e que se considera premente, face ao Estado da Arte.

No final desta fase, foram analisados os resultados e foi feita a sua discussão, possibilitando a apresentação das conclusões e a obtenção de contributos para o conhecimento, bem como limitações e recomendações.

3. Ordenamento jurídico aplicável à videovigilância policial

3.1 Normativos europeus

A Estratégia da UE para a Segurança, que tem por fim último proteger os cidadãos e promover o modo de vida europeu, estabelece como pilares estratégicos, para o período de 2020 a 2025, o ambiente de segurança, a resposta a ameaças em constante evolução, a proteção do terrorismo e da criminalidade organizada e um ecossistema de segurança europeu sólido (CE, 2020a).

O documento alude ao facto de os benefícios inerentes à globalização, à livre circulação e à transformação digital comportarem, igualmente, riscos e custos, podendo ser facilitadores do terrorismo e da criminalidade organizada e representar ameaças cada vez mais complexas e difusas à segurança (CE, 2020a).

Esta Estratégia sublinha, ainda, que a segurança e o respeito pelos DLG não são objetivos incompatíveis, mas sim complementares, devendo constituir o desiderato de uma política assente nos valores comuns europeus (CE, 2020a).

Ao nível da proteção dos espaços públicos, dá ênfase à premência de a reforçar com sistemas de deteção adequados, considerando que os mais recentes ataques terroristas se centraram nestes locais, sem, contudo, prejudicar as liberdades dos cidadãos (CE, 2020a).

No domínio da salvaguarda dos DLG, denota-se uma especial preocupação para a promoção do intercâmbio de experiências e boas práticas no reforço dos meios para a proteção dos espaços públicos, integrando os vários setores, público e privado, que deve dar primazia à sensibilização, requisitos de desempenho e testes dos equipamentos de deteção, bem como à verificação de antecedentes para fazer face às ameaças, salvaguardando o facto de minorias e pessoas vulneráveis, devido à religião ou ao género, poderem ser afetadas de forma desproporcionada, o que exigirá atenção e medidas especiais (CE, 2020a).

A Carta dos Direitos Fundamentais da UE estabelece, de forma geral, que todos os cidadãos têm o direito à proteção de dados pessoais e ao respeito pela vida privada (UE, 2012).

Na garantia deste direito, têm sido implementadas medidas que visam a proteção de dados, tendo, em 25 de maio de 2018, entrado em vigor o Regulamento UE n.º 2016/679, Regime Geral de Proteção de Dados (RGPD), regulador do tratamento de dados pessoais e da livre circulação desses dados, com vista a uniformizar os diversos sistemas nacionais (CE, 2016).

O RGPD estabelece as regras relativas ao tratamento, por uma pessoa, empresa ou organização, de dados pessoais relativos a pessoas, na UE, definindo novos procedimentos do ponto de vista tecnológico, no quadro do reforço da proteção jurídica dos direitos dos titulares dos dados (Presidência do Conselho de Ministros, 2022).

No contexto da videovigilância policial, assume preponderância a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, relativa ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho (no domínio da cooperação judiciária em matéria penal e da cooperação policial).

Em 2020, a CE emitiu o Livro Branco da IA, que apresenta opções políticas para um desenvolvimento fiável e seguro desta tecnologia na Europa, no respeito pelos DLG dos cidadãos (CE, 2020b, p. 3). Este documento refere ser essencial que as administrações públicas, assim como outros domínios de interesse público, utilizem, na prossecução das suas atividades, produtos e serviços baseados em IA (CE, 2020b, p. 9).

Em 2021, foi elaborada a proposta de regulamento do PE e do Conselho, proposta de regulação europeia 2021/006 (COD), com vista a estabelecer regras harmonizadas em matéria de IA, alterando atos legislativos, no desiderato de preservar a liderança tecnológica e assegurar que novas tecnologias, desenvolvidas no respeito pelos valores, DLG e princípios da UE, estejam ao serviço dos cidadãos (CE, 2021).

O Livro Branco da IA visa promover a adoção de IA e abordar os riscos associados a determinadas utilizações, pretendendo a proposta de regulamento referida dar corpo ao segundo objetivo, através do desenvolvimento de um ecossistema de confiança sustentado num quadro jurídico para uma IA de confiança (CE, 2021). Neste domínio, foram produzidas conclusões que reforçam a importância de dar resposta a desafios como a opacidade, a complexidade, os preconceitos, um certo grau de imprevisibilidade e autonomia parcial de determinados sistemas de IA, para garantir a compatibilidade destes com os DLG e facilitar a aplicação das normas jurídicas (CE, 2021).

3.2 Transposição nacional

Relativamente à videovigilância policial, no cômputo nacional, foi inicialmente regulada através da Lei nº 1/2005, de 10 de janeiro, com alterações posteriores, introduzidas pela Lei nº 39-A/2005, de 29 de julho, pela Lei nº 53-A/2006, de 29 de dezembro, e pela Lei nº 9/2012, de 23 de fevereiro, normativos que enquadravam a utilização destes sistemas pelas

FS em locais públicos de utilização comum, para captação e gravação de imagem e som e seu posterior tratamento (Assembleia da República [AR], 2012).

O Relatório Anual de Segurança Interna (RASI) de 2011 salienta a importância e a crescente utilização de sistemas de videovigilância para a proteção de pessoas e bens, com vista à garantia de melhores condições para a prevenção e repressão da criminalidade em espaços públicos, de que resultou o reforço dos normativos jurídicos para proteção dos dados pessoais, com a publicação, em 2012, da terceira alteração à Lei nº 1/2005, de 10 de janeiro (Sistema de Segurança Interna [SSI, 2012], p. 120).

Este enquadramento legal estabeleceu que o início do procedimento de autorização para a instalação dos equipamentos tem lugar por requerimento do dirigente máximo da FS com jurisdição na área de observação ou pelo respetivo Presidente de Câmara Municipal, em processo acompanhado pelo conjunto de elementos que fundamentam as condições de instalação e mediante parecer não vinculativo da Comissão Nacional de Proteção de Dados (CNPD).

As Portarias n.º 372/2012 e n.º 373/2012, ambas de 16 de novembro, vieram regulamentar a utilização de câmaras de vídeo pelas FS em locais públicos de utilização comum, designadamente sobre os requisitos técnicos e simbologia (AR, 2012).

As Leis n.º 58/2019 e n.º 59/2019, ambas de 8 de agosto, fizeram a transposição nacional do RGPD e da Diretiva (UE) 2016/680, respetivamente (AR, 2019).

Entrou, entretanto, em vigor a Lei n.º 95/2021, de 29 de dezembro, que veio substituir e revogar a Lei nº 1/2005, de 10 de janeiro, e que regula a utilização e o acesso a sistemas de videovigilância, para captação, gravação e tratamento de imagem e som (AR, 2021).

3.3 Controlo e fiscalização

Foi constituído o Comité Europeu para a Proteção de Dados (CEPD), através do RGPD, que é composto por representantes das autoridades nacionais para a proteção de dados dos Estados-Membros da UE e pela Autoridade Europeia de Proteção de Dados, que, essencialmente, aprova diretrizes, recomendações e boas práticas, assim como emite decisões vinculativas com vista ao controlo da coerência na aplicação do RGPD (CNPD, 2022).

Ao nível nacional, a autoridade de controlo é a CNPD, responsável pela fiscalização do cumprimento do RGPD e dos normativos vigentes, designadamente os referidos nos pontos anteriores deste capítulo (CNPD, 2022).

3.4 Síntese conclusiva

Ao nível comunitário, está em vigor o RGPD e a Diretiva (UE) 2016/680, assumindo a segunda preponderância, no contexto da videovigilância policial, sendo reguladora do tratamento de dados pessoais para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e da livre circulação desses dados.

Encontra-se em análise e discussão, pelos Estados-Membros, a proposta de Regulamento 2021/006 (COD), com vista a estabelecer regras harmonizadas em matéria de utilização de IA, dando corpo ao segundo objetivo do Livro Branco, para o desenvolvimento de um ecossistema fiável sustentado num quadro jurídico para uma IA de confiança – respondendo a desafios como a opacidade, a complexidade, os preconceitos, um certo grau de imprevisibilidade e autonomia parcial de determinados sistemas de IA, com o fim de garantir a compatibilidade destes com os DLG e facilitar a aplicação das normas jurídicas.

No cômputo nacional, decorrente do quadro jurídico comunitário, encontra-se em vigor a Lei n.º 95/2021, de 29 de dezembro, reguladora da utilização e do acesso a sistemas de videovigilância, para captação, gravação e tratamento de imagem e som, assim como as Leis n.º 58/2019 e n.º 59/2019, ambas de 8 de agosto, em transposição do RGPD e da Diretiva (UE) 2016/680, respetivamente, e, ainda, as Portarias n.º 372/2012 e n.º 373/2012, ambas de 16 de novembro, que regulamentam a utilização de câmaras de vídeo pelas FS, em locais públicos de utilização comum, designadamente os requisitos técnicos e simbologia.

Relativamente ao controlo e fiscalização, ao nível europeu, foi constituído o CEPD, composto por representantes das autoridades nacionais para a proteção de dados dos Estados-Membros da UE e pela Autoridade Europeia de Proteção de Dados. A nível nacional, a autoridade de controlo é a CNPD, sendo responsável pela fiscalização do cumprimento do RGPD e demais normativos vigentes.

Considera-se, assim, respondida a QD1, relativa ao ordenamento jurídico aplicável à videovigilância policial em espaços públicos, no contexto europeu, e a sua transposição nacional.

4. Aplicação de Inteligência Artificial nos sistemas de videovigilância policial

4.1 Implementação pela GNR

Neste subcapítulo é analisada a aplicabilidade de IA em sistemas de videovigilância policial implementados pela GNR em espaços públicos, assim como os critérios, requisitos técnicos e medidas a salvaguardar para a autorização de instalação e utilização, com base em documentação institucional, nas entrevistas realizadas aos níveis político, institucional e técnico (SEAAI, GNR e Motorola *Solutions*, respetivamente) e no parecer emitido pela CNPD para o sistema de videovigilância policial de Albufeira, o mais recentemente submetido a aprovação (considerando que esta entidade não concedeu entrevista).

As entrevistas permitiram complementar a análise documental, nomeadamente de legislação, com informação adicional, que não está disponível de outra forma e que é essencial à investigação.

Considerando que o processo para implementação de sistemas de videovigilância inicia com a instrução do respetivo pedido de autorização, torna-se pertinente referir em concreto os elementos que deve contemplar, conforme previsto no ordenamento jurídico vigente e sumarizados em Quadro 2:

Quadro 2 – Elementos do pedido de autorização para instalação de sistemas de videovigilância

Diploma	Elementos
Lei n.º 95/2021, de 29 de dezembro **(art.º 6º)**	– Fundamentação da necessidade; – Identificação do local e área abrangidos pela captação e dos pontos de instalação das câmaras; – Características técnicas do equipamento; – Identificação da FS responsável pela conservação e tratamento dos dados; – Procedimentos de informação ao público sobre a existência do sistema; – Descrição dos critérios do sistema de gestão analítica dos dados captados; – Mecanismos para assegurar o correto uso dos dados registados; – Avaliação de impacto do tratamento de dados sobre a proteção de dados pessoais.
Lei n.º 59/2019, de 8 de agosto **(art.º 29º)**	(Avaliação de Impacto) – Descrição geral das operações de tratamento de dados pessoais; – Avaliação dos riscos para os DLG dos titulares dos dados; – Medidas para mitigar os riscos; – Garantias, medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais e demonstrar a conformidade do tratamento.

Fontes: Lei n.º 95/2021, de 29 de dezembro, e Lei n.º 59/2019, de 8 de agosto.

4.1.1 Análise pelo nível político

No domínio da segurança interna, a aplicação de IA nos sistemas de videovigilância policial "só pode ser entendida como um contributo para a salvaguarda dos direitos dos

cidadãos, nomeadamente na salvaguarda do direito à segurança, cuja garantia é uma tarefa fundamental do Estado" (Gabinete SEAAI, entrevista, 25.03.2022). Neste particular, devem ser observados os princípios constitucionais, nomeadamente o da proporcionalidade, para salvaguardar que a utilização não seja violadora dos direitos fundamentais que se visa proteger (SEAAI, *op. cit.*).

Na Lei n.º 95/2021, de 29 de dezembro, é admissível "o tratamento de dados ter subjacente um sistema de gestão analítica de dados, por aplicação de critérios técnicos, de acordo com os fins a que se destinam os sistemas" (SEAAI, *op. cit.*). Neste desiderato, aquando da submissão do pedido de autorização para a implementação dos sistemas de videovigilância, deve ser obrigatoriamente incluída "a descrição dos critérios técnicos utilizados no sistema de gestão analítica dos dados captados", no pressuposto de que devem ser previamente definidos e autorizados e objeto de parecer obrigatório da CNPD (SEAAI, *op. cit.*).

Os critérios e pressupostos técnicos devem ser definidos e adaptados a cada um dos fins a que se destinam, tendo obrigatoriamente que salvaguardar os princípios constitucionais e a proteção de dados (SEAAI, *op. cit.*). Neste domínio, será publicada a regulamentação da Lei n.º 95/2021, de 29 de dezembro, "sendo expectável que essa regulamentação venha trazer orientações sobre os requisitos técnicos que a solução analítica de dados deve observar" (SEAAI, *op. cit.*).

Torna-se, assim, pertinente analisar a evolução da *Analítica de Vídeo* e as possibilidades de aplicação, neste contexto, bem como alguns conceitos complementares, que se incluem em Apêndice B.

O parecer da CNPD para o sistema de videovigilância policial de Albufeira refere que o pedido é omisso quanto aos critérios de utilização desta tecnologia (IA), não estando definidas as regras (de uso) mas apenas funcionalidades ou potencialidades da câmara, assim como salienta que a utilização de analítica de vídeo por recurso a IA, sem especificação dos termos e condições de tal utilização, não salvaguarda o rastreamento de cidadãos sem garantias de não discriminação e em proporcionalidade (CNPD, 2021).

O parecer elenca, ainda, situações que, não sendo salvaguardadas, tornam o sistema de risco elevado, apresentando recomendações para a segurança do sistema e para a proteção dos DLG conforme incluído em Quadro 3:

Quadro 3 – Recomendações da CNPD para a segurança dos sistemas e proteção dos DLG dos cidadãos

Recomendações	Descrição
Segregação física e lógica das redes de videovigilância	Aplicação de protocolo HTTPS, para segregação das outras redes.
Inclusão de sistema anti-tampering nos armários de comunicações	Sistema com alertas, a ser implementado para além de outros, nomeadamente plataformas de software que habilitem acompanhar o estado dos equipamentos que interagem, como as câmaras (Site Health).
Resguardo dos armários de comunicações	Localização dos armários de comunicações em pontos que dificultem o acesso, nos locais públicos.
Registo de todas as ações efetuadas no sistema e garantia da integridade	Registo de todas as ações efetuadas por um utilizador, incluindo tentativas de acesso, assim como a obrigação de garantia da sua integridade, através de assinatura e TimeStamp.
Garantia da disponibilidade dos dados em caso de eliminação acidental	Garantia da disponibilidade dos dados, no prazo dos 30 dias, em caso de eliminação acidental, para além das condições previstas para a sua recuperação, em caso de avarias no armazenamento.
Quantificação de dois servidores para garantia da continuidade do sistema	Quantificação de dois servidores, em cenário de failover, com a arquitetura de partilha da unidade dedicada a armazenamento de dados, assegurando, assim, a continuidade do sistema, em caso de falha no servidor ativo.
Registo dos acessos à(s) sala(s) de tratamento de dados	Registo de entradas e saídas, no sentido de se poder demonstrar a imputabilidade de qualquer evento.
Garantia da Auditabilidade do sistema	Garantia de auditabilidade do sistema e dos mecanismos de proteção.

Fonte: CNPD (2021).

Consta, ainda, como essencial, a predefinição das circunstâncias (caracterização das situações), que justificam a necessidade da utilização do algoritmo de análise das imagens, à luz das finalidades do sistema (e do tratamento dos dados), assim como os critérios ou fatores que podem estar na base da seleção das pessoas ou veículos para rastreamento (CNPD, 2021).

4.1.2 Análise pelo nível institucional e técnico

A GNR tem procurado incorporar as melhores práticas desenvolvidas pelas organizações inovadoras, tanto nacionais como internacionais, tendo como centro de gravidade as Pessoas (GNR, 2020a, p. 4).

No cerne das preocupações encontram-se as ameaças e os riscos à Segurança, cada vez mais globais, diversificados, complexos e sofisticados (GNR, 2020a, p. 42). De acordo com as orientações estratégicas, são impostas linhas de atuação claras, minimizando e ultrapassando as dificuldades existentes (GNR, 2020b, Nota Prévia).

A GNR implementa sistemas de videovigilância em espaços públicos, na sua área de responsabilidade, com vista à manutenção da ordem e segurança públicas, assim como à prevenção e dissuasão da prática de crimes (Serrão, entrevista, 08.04.2022).

Relativamente aos equipamentos, devem as suas especificações, do ponto de vista técnico, identificar corretamente a forma de recolha, transmissão e conservação das imagens, nomeadamente as características que permitam o elencado em Quadro 4:

Quadro 4 – Exemplos de especificações técnicas dos equipamentos dos sistemas da GNR, no âmbito da recolha, transmissão e conservação das imagens

Especificações	Descrição
Utilização exclusiva	Utilização exclusiva da FS, no que respeita ao controlo, domínio e gestão do sistema.
Perfis de acesso	Acesso ao sistema mediante a atribuição de perfis de acesso.
Encriptação das imagens	Imagens encriptadas desde a câmara até à visualização, pelo militar.
Software para proteção de locais privados	Utilização de software para bloquear a captação de locais privados, como janelas e portas de edifícios, em especial o seu interior.
Impossibilidade de criação de Perfis	Garantia que o sistema tem a impossibilidade de criar perfis, para salvaguarda da discriminação de pessoas.
Meios físicos para gravação dos dados	Gravação dos dados apenas em meios físicos exclusivos para esse efeito.
Registo nos dados	Inscrição, nos dados, de forma inequívoca, da data, hora e local da captação.
Conservação dos dados em registo codificado	Conservação dos dados em registo codificado, pelo prazo máximo legalmente previsto, de 30 dias, contados a partir da respetiva captação.

Fonte: Serrão, *op. cit.* (2022).

Adicionalmente, é salientado que,

> […] Caso exista recurso a analítica de vídeo, deve existir um conjunto de regras para os utilizadores deste tipo de tecnologia, no sentido de limitar a criação de perfis e o risco de discriminação e de violação do art.º 6 da Lei 59/2019 […] assim como formação específica. Importa que exista um conjunto de critérios e quem é o responsável pela definição de regras a aplicar. (Serrão, *op. cit.*)

De acordo com Pessoa (entrevista, 29.03.2022), entre os requisitos a salvaguardar nos sistemas e exemplos de boas práticas, salientam-se os contantes em Quadro 5:

Quadro 5 – Análise pelo nível técnico aos requisitos e boas práticas a salvaguardar nos sistemas com IA

Sistemas de videovigilância com IA	
Requisitos	– Cumprimento da legislação em vigor; – Formação a todos os operadores do sistema; – Auditoria dos elementos adstritos a esta função; – Decisão final humana (operador e supervisor).
Boas práticas	– Gestão por operadores e supervisores certificados; – Investigação e/ou extração de imagens mediante dupla autenticação (senha e QR code) - operador e supervisor, de forma presencial; – Auditabilidade do sistema, de 6 em 6 meses, por entidade de segurança, com foco principal: o Na gestão do sistema instalado e se cumpre a legislação vigente; o Nas infraestruturas físicas (cablagens) e de ligação de ativos de redes e sua forma de conexão, para certificar que o canal captação-gravação-gestão (operação do sistema) se mantém inviolável e encriptado; o Na inalteração do autorizado, em matéria de utilização. – Registos auditáveis, dentro do limite legal de 30 dias, por entidades credenciadas, de forma aleatória ou programada (dados devem permanecer consistentes e invioláveis); – Sistema integral de um fabricante, para facilitar a gestão e auditoria, bem como as definições de segurança, evitando a inviabilização da responsabilização; – Base de dados própria e encriptada (não deverá ser SQL, pelas vulnerabilidades), em que a gestão, controlo e domínio sejam exclusivos à FS; – Sistema operativo baseado em Linux, promovendo a inviolabilidade dos dados, na medida em que não serão visíveis em caso de ataques cibernéticos.

Fonte: Pessoa, *op.cit.* (2022).

Quanto aos critérios em aplicação, não contemplam o tratamento de *metadados*, e, assim, não permitem identificar de forma inequívoca uma pessoa e correlacioná-la num determinado período de tempo (Pessoa, *op. cit.*). Os dados são arquivados com uma encriptação fotograma a fotograma, compondo uma determinada imagem sem descrição e sem vínculo bidirecional, vínculo que será apenas atribuído quando o operador e/ou supervisor do sistema acionarem uma "pesquisa", sendo o resultado a apresentação de diversas imagens semelhantes, mas não vinculativas, cabendo ao operador e/ou supervisor

fazer sempre a identificação afirmativa e continuar (ou não) a pesquisa/investigação, da mesma forma que o faria "no terreno", tornando, assim, a gestão dos dados não vinculativa e não violável (Pessoa, *op. cit.*).

4.2 Perspetiva de Forças de Segurança congéneres europeias

Neste subcapítulo é analisada a aplicação de IA em sistemas de videovigilância policial em espaços públicos, por FS congéneres europeias, concretamente a GC, a GN, a AC e a MH, numa ótica de *benchmarking*, assim como a sua perspetiva relativamente à temática. A análise teve por base documentação institucional e os resultados de entrevistas a Oficiais destas FS, com funções e experiências relevantes para o estudo em apreço, cuja matriz de análise está vertida em Apêndice C.

Antes de apresentar a perspetiva de cada FS congénere, resulta pertinente salientar o seguinte:

- As cinco FS congéneres, onde se inclui a GNR, realizam ações de policiamento orientado pela análise de informações policiais, utilizam sistemas informáticos no domínio da recolha e da análise de dados, elaboram relatórios de informações e mapas de risco da criminalidade, assim como utilizam sistemas informáticos de informações criminais interoperáveis com outras entidades no setor da Segurança, ao nível nacional, para partilha de informação;
- Na senda, todas consideram que tais ações de policiamento promovem a rentabilização dos recursos policiais, e, quatro destas, consideram que, nos locais de incidência, a taxa de criminalidade diminui;
- Relativamente à videovigilância policial, quatro confirmaram implementar esses sistemas em espaços públicos, nas respetivas áreas de responsabilidade, apesar de apenas uma (AC) ter referido aplicar IA, com conexão a bases de dados de informações criminais;
- Todas transmitiram a sua perspetiva nacional e institucional, sendo possível aferir que consideram que a implementação de videovigilância policial em espaços públicos pode contribuir para a capacidade preditiva e que a aplicação de IA nestes sistemas aduz mais-valias, mas, também, a necessidade de assegurar garantias, medidas de segurança e mecanismos para assegurar a proteção de dados pessoais e a conformidade do tratamento dos dados, decorrente do ordenamento jurídico em vigor.

4.2.1 *Guardia Civil* Espanhola

É responsável por cerca de 84% do território espanhol e das águas territoriais, salientando-se, no contexto, a proteção das redes de comunicação, portos e aeroportos (FIEP, 2022a).

De acordo com a GC, a globalização e a revolução tecnológica são, atualmente, inseparáveis, devendo as FS adaptar as suas metodologias e técnicas de investigação, à luz desta nova realidade (FIEP, 2022b).

Aludindo ao uso da IA, a congénere salienta as restrições legais existentes, fazendo menção à proposta de regulamento do PE para harmonizar as regras de utilização, que contempla práticas proibidas e determinadas exceções, propondo salvaguardas específicas, designadamente sobre o uso de sistemas de identificação biométrica remota, e estabelecendo um cenário de tecnologias e sistemas de risco elevado para os DLG dos cidadãos, para os quais deverão ser observados requisitos obrigatórios e procedimentos aprovados, para que possam ser implementados na UE (FIEP, 2022b).

A GC possui todas as capacidades para ser considerada polícia integral, encontrando-se a integrar a IA gradualmente nestas, com vista a facilitar a sua atividade diária (FIEP, 2022b).

Apesar de implementar sistemas de videovigilância policial em espaços públicos, na sua área de responsabilidade, não aplica, ainda, a IA para tratamento e análise dos dados (Mestre, entrevista, 08.02.2022). Neste domínio, considera a aplicação de IA como uma mais-valia, referindo que a videovigilância e a conexão com bases de dados criminais (europeus e nacionais) potenciaria a eficácia das Agências de Aplicação da Lei (Mestre, *op. cit.*).

Sobre as especificações técnicas dos equipamentos de videovigilância, no âmbito do tratamento e análise de dados e para salvaguarda da privacidade das pessoas e os seus DLG, a legislação nacional espanhola estabelece que a resolução autorizadora deve incluir os recursos das câmaras, não existindo, contudo, uma relação definida para os recursos mínimos específicos (Mestre, *op. cit.*). Neste particular, é desenvolvida uma avaliação do impacto das operações de tratamento de dados dos cidadãos, incluindo as medidas mitigadoras dos riscos identificados, em conformidade com a legislação vigente (Mestre, *op. cit.*).

Para qualquer atividade de processamento de dados, a GC assegura as garantias, medidas de segurança e mecanismos para assegurar a proteção de dados pessoais e a conformidade do tratamento, assim como presta informação aos cidadãos sobre a Entidade

responsável pelos direitos de acesso e eliminação, conforme decorre da transposição nacional da Diretiva 680/2016 (Mestre, *op. cit.*).

Considerando que a implementação de videovigilância policial em espaços públicos maximiza a atuação policial e pode contribuir para a capacidade preditiva, a GC tem projetos para adotar o modelo de policiamento preditivo, embora ainda não se encontrem em prática (Mestre, *op. cit.*).

A congénere utiliza como principal sistema informático, no domínio das informações policiais, o Sistema SIGO (*Sistema Integrado de Gestión Operativa*), em que são registados todos os eventos, tarefas, relatórios de ocorrências e serviços e que inclui interface de pesquisa (Mestre, *op. cit.*). Apesar de considerar que a ligação destes sistemas a bases de dados de informações criminais traria mais-valias, potenciando, nomeadamente, a localização de pessoas desaparecidas, de vítimas de crimes e pessoas com medidas restritivas, a GC não tem o SIGO ligado a nenhuma base de dados desta natureza (Mestre, *op. cit.*).

O SIGO elabora mapas de risco da criminalidade, considerando que os eventos são geolocalizados e possuem marca de tempo, sendo as ações de policiamento orientadas pela análise de informações policiais, com análise de estatísticas aos níveis central e local, para avaliação dos riscos e ameaças (Mestre, *op. cit.*). É, neste domínio, indicada a diminuição da taxa de criminalidade nos locais de incidência do referido policiamento, sendo considerado que promove a rentabilização dos recursos policiais (Mestre, *op. cit.*).

4.2.2 *Gendarmerie Nationale* Francesa

É responsável por cerca de 95% do território francês (FIEP, 2022a). No quadro das missões administrativas, cerca de 40% das atividades desenvolvidas são dedicadas à proteção de pessoas e bens (FIEP, 2022a).

No contexto dos impactos da globalização, reforça a necessidade de explorar a digitalização, a IA e a automatização para otimizar as tarefas humanas, assim como a premência de assegurar infraestruturas de dados fiáveis, indicando como pré-requisitos a antecipação e a centralização (FIEP 2022b).

A congénere não implementa sistemas de videovigilância policial em espaços públicos, na sua área de responsabilidade, embora considere uma mais-valia a sua utilização, em casos específicos (grandes eventos), em espaço e tempo limitados (Perrot, entrevista, 08.02.2022).

Aplica a IA no desenvolvimento de ferramentas para otimizar a atividade policial, nomeadamente para análise preditiva, para antecipar as ocorrências e evitar o efeito *black box* (Perrot, *op. cit.*).

Adotando o modelo de policiamento preditivo, utiliza sistemas informáticos de informações policiais baseados na obtenção de dados – análise preditiva, autenticação *deepfake* e reconhecimento de discurso (este último, ainda em desenvolvimento), assim como elabora mapas de risco da criminalidade, através de sistemas automáticos de análise preditiva (Perrot, *op. cit.*).

No contexto das ações de policiamento orientado pelas informações policiais, é salientada a importância de manter a decisão humana, a par da utilização dos sistemas automáticos (Perrot, *op. cit.*). Neste quadro, confirma a diminuição da taxa de criminalidade, como resultado destas ações de policiamento, indicando, no entanto, a importância de associar uma análise ao impacto das ações de prevenção e de repressão nesses locais (Perrot, *op. cit.*).

A GN utiliza, também, sistemas informáticos de informações criminais, interoperáveis ao nível nacional, para partilha de informações, ainda que de forma limitada, por restrições relacionadas com aspetos legais (Perrot, *op. cit.*).

4.2.3 *Arma dei Carabinieri* Italiana

É responsável pela ordem e segurança públicas em todo o território italiano (FIEP, 2022a).

À luz da globalização e do desenvolvimento tecnológico, implementou, no seu Comando-Geral, uma Divisão especialmente dedicada à pesquisa e desenvolvimento de novas tecnologias, incluindo IA (FIEP, 2022b). Salienta, neste domínio, como boas práticas, acompanhar a inovação tecnológica, partilhar informação entre FS congéneres e observar as restrições impostas por Lei (FIEP, 2022b). Um exemplo apontado é a utilização legal da IA para efeitos de investigação, em Itália, sendo que os regulamentos não permitem a utilização dos resultados dos algoritmos de forma direta, sem validação prévia por operadores humanos (FIEP, 2022b).

Implementando sistemas de videovigilância policial em espaços públicos, indicou utilizar IA para tratamento e análise dos dados, referindo, ainda, que tal maximiza a atuação policial e pode contribuir para a capacidade preditiva (Servedio, entrevista, 30.03.2022). A congénere referiu que os sistemas estão ligados a bases de dados de informações criminais,

ressalvando que foram renovados e implementados muito recentemente e são centrados nas necessidades de investigação (Servedio, *op. cit.*).

Neste âmbito e no que se refere à utilização de aplicações de identificação de perfis suspeitos, de análise de movimentos e deteção de padrões suspeitos e/ou de controlo de tráfego, a congénere indicou que, no momento, não faz, mas que poderá vir a fazer, dentro dos limites da Lei (Servedio, *op. cit.*). A utilização é considerada uma mais-valia, na medida em que pode baixar a taxa de falsos positivos, assegurar uma curva característica de funcionamento do recetor aceitável e permitir matriz de confusão em cenários de ambiente de elevada concentração de pessoas (Servedio, *op. cit.*).

Na implementação dos sistemas é desenvolvida uma avaliação do impacto das operações de tratamento de dados pessoais, em cumprimento do RGPD, assim como são asseguradas as garantias, medidas de segurança e mecanismos para a proteção de dados pessoais e a conformidade do tratamento (Servedio, *op. cit.*). Neste sentido, está definida, ao nível da congénere, uma entidade responsável pelo exercício dos direitos de acesso e retificação dos dados, assim como é feita a comunicação à Autoridade responsável, em transposição da regulamentação europeia (Servedio, *op. cit.*).

A AC não adota o modelo de policiamento preditivo, mas realiza ações de policiamento orientado pelas informações policiais e utiliza sistemas informáticos no domínio da recolha desse tipo de informação, integrando dados de domínio transversal, relatórios de crime e análise de estatísticas de crime (Servedio, *op. cit.*). Elabora relatórios de informações e mapas de risco da criminalidade, ressalvando que se trata de uma função conjunta (partilhada) e que são utilizados sistemas informáticos de informações criminais interoperáveis ao nível nacional, com outras Entidades no setor da Segurança (Servedio, *op. cit.*).

4.2.4 *Marechaussee* Holandesa

É responsável pela segurança pública no Reino dos Países Baixos, incluindo os territórios no Caribe, encontrando-se implantada nos locais de importância estratégica, com especial ênfase às instalações reais, à fronteira externa da UE e aeroportos (FIEP, 2022a).

Encontra-se a trabalhar na inovação tecnológica por experimentação, reunindo conhecimento, designadamente, no domínio da IA, em estreita colaboração com centros de estudo, universidades e agências governamentais (FIEP, 2022b). Neste particular, de referir o desenvolvimento de visão computacional baseada em IA, com a experimentação da designada deteção comportamental (*behavior detection*) para detetar automaticamente

comportamentos humanos indesejados ou anormais, em filmagens de câmaras, que poderão possibilitar antecipar um ataque e acionar meios e desenvolver medidas por parte das FS (FIEP, 2022b). Como exemplo, é indicado comportamento de *searching*, cujos indicadores poderão constituir captura de imagens de residências de entidades importantes, passagem recorrente de pessoas e/ou veículos desconhecidos, de forma suspeita, ou intrusão em perímetros (FIEP, 2022b).

A congénere implementa sistemas de videovigilância policial em espaços públicos, nomeadamente nos aeroportos, referindo, no entanto, que ainda não aplica IA para tratamento e análise dos dados (van Staveren, entrevista, 08.02.2022). Neste contexto, indica que os dados são armazenados em sistema seguro e automaticamente eliminados após um número de dias definido, assim como é feita uma avaliação do impacto de privacidade, para salvaguardar os DLG dos cidadãos, estando a ser desenvolvidos métodos de anonimização para imagens de vídeo, como meio de proteção da privacidade (van Staveren, *op. cit.*).

A MH assegura, ainda, medidas para que o acesso a dados pessoais seja estritamente controlado, apenas possível a quem esteja autorizado e tenha a necessidade operacional de o fazer – tais dados apenas poderão ser armazenados para efeitos de investigação, mediante fundamento legal (van Staveren, *op. cit.*).

Está definida, ao nível da congénere, uma entidade para assegurar o exercício dos direitos de acesso e retificação dos dados, tendo desenvolvido, relativamente à IA, um manifesto ético, com as diretrizes éticas seguidas e a especificação das possíveis questões neste domínio, com base nos regulamentos europeus, num trabalho desenvolvido em estreita colaboração com juristas experientes na área da análise de dados para fins policiais (van Staveren, *op. cit.*).

A MH reforça a utilização de sistemas de videovigilância policial em espaços públicos com aplicação de IA como uma mais-valia, na medida em que permite potenciar a deteção de padrões suspeitos, com valor acrescentado na previsão e prevenção de criminalidade grave (van Staveren, *op. cit.*). Encontra-se a desenvolver e experimentar protótipos de aplicações de identificação de perfis de suspeitos, de análise de movimentos e deteção de padrões suspeitos e/ou de controlo de tráfego (van Staveren, *op. cit.*).

De referir, adicionalmente, que realiza ações de policiamento orientado pelas informações policiais, ainda que de forma limitada, que produz relatórios sobre as tendências dos fenómenos criminais e que utiliza sistemas informáticos de informações criminais

interoperáveis com outras entidades, ao nível nacional, apesar de apontar que, por vezes, com acesso limitado a outros sistemas (van Staveren, *op. cit.*).

Sobre a recolha de informações policiais, é obtida através dos operacionais e em colaboração com outras organizações, no domínio da Segurança, adotando a MH o modelo de policiamento preditivo, num alcance muito limitado, com recurso, nomeadamente, a informação proveniente de fontes abertas, para previsão de eventos e para otimizar o planeamento e emprego dos meios policiais – num horizonte temporal de dois dias a duas semanas (van Staveren, *op. cit.*).

4.3 Síntese conclusiva

A Lei n.º 95/2021, de 29 de dezembro, admite que o tratamento de dados tenha subjacente um sistema de gestão analítica de dados, por aplicação de critérios técnicos, de acordo com os fins a que se destinam os sistemas, os quais devem ser incluídos no pedido de autorização para a implementação, para serem previamente definidos e autorizados, mediante parecer obrigatório da CNPD.

No que se refere à aplicação de IA, os critérios concretos para a utilização desta tecnologia devem ser especificados no pedido, apesar de, neste domínio, se aguardar a publicação da regulamentação a esta Lei, que trará orientações sobre os requisitos técnicos que a solução analítica de dados deve observar.

A analítica de vídeo tem diversas possibilidades de aplicação, incluindo o recurso a IA, tendo por base algoritmos, mais ou menos evolutivos, que podem funcionar de diversas formas, dependendo do que se pretende analisar, que possibilitam analisar elevados volumes de imagens, criando um tipo de ação ou alerta e potenciar as operações de segurança.

A GNR, na implementação de sistemas de videovigilância policial, salvaguarda todas as garantias e mecanismos para a proteção de dados pessoais, não aplicando, ainda, a IA, apesar das mais-valias e do interesse que lhe reconhece, tendo, no último pedido autorizado, a CNPD salientado a necessidade (para utilização de IA) da especificação dos critérios de uso e da predefinição das circunstâncias – caracterização das situações – que justifiquem o recurso ao algoritmo de análise de imagens, incluindo os critérios ou fatores na base da seleção de pessoas e/ou veículos para rastreamento.

Respondendo-se à QD2, conclui-se que a GNR pode, numa perspetiva legal e técnica, em cumprimento do ordenamento jurídico em vigor, aplicar IA nos sistemas de videovigilância em espaços públicos, não obstante essa aplicação carecer de um parecer obrigatório da CNPD.

Relativamente às FS congéneres europeias, respondendo-se à QD3, apenas a AC confirmou aplicar IA nos seus sistemas de videovigilância em espaços públicos. Não obstante, foi possível reunir a perspetiva de todas, sendo unânime o reconhecimento das mais valias aduzidas da sua utilização, nomeadamente, a capacidade preditiva e a maximização da atuação policial. Esta utilização terá que ser conjugada com a necessidade de asseverar garantias, medidas e mecanismos de segurança para a proteção de dados pessoais e a conformidade do tratamento, segundo o ordenamento jurídico em vigor.

5. Discussão de resultados

Congregando a análise dos resultados, é possível responder à QC, para elencar um conjunto de boas práticas para aplicar IA em sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor.

Das entrevistas realizadas às congéneres, extrai-se como ideias chave a importância de manter a decisão humana (a par da utilização de sistemas automáticos), o permanente acompanhamento da evolução tecnológica, a partilha de informação entre FS, a observação dos normativos legais (especialmente restrições), a validação prévia dos resultados dos algoritmos por operadores humanos, o desenvolvimento de métodos de anonimização para as imagens de vídeo e o desenvolvimento de um manifesto ético relativamente à IA, com as diretrizes éticas seguidas e especificadas as possíveis questões neste domínio, com base nos regulamentos europeus e num trabalho que envolva colaboração com juristas experientes na área da análise de dados para fins policiais.

Para fundamentar a necessidade de utilização de sistemas com IA, consideram-se pertinentes as mais-valias e potencialidades indicadas pelas FS congéneres, tendo sempre por referência, conforme salientado pelo nível político, que concorrerão para o bem jurídico superior, a Segurança, fim último da utilização destes sistemas. Estas mais-valias e potencialidades são esquematizadas em figura 1:

Figura 1 – Mais-valias e potencialidades de um sistema de videovigilância policial com IA
Fonte: Entrevistas nível institucional (2022).

Da análise das entrevistas ao nível político e técnico, assim como da Lei n.º 95/2021, de 29 de dezembro, aduz-se que a implementação dos sistemas depende da *instrução do pedido de autorização e utilização*, que é submetido à Tutela.

Neste desiderato, considera-se que o processo de implementação se materializa na instrução deste pedido, em três domínios, que se correlacionam em torno dos princípios basilares que devem nortear a utilização desta tecnologia, face aos fins a que se destina (necessidade, proporcionalidade e transparência), conforme ilustrado em Figura 2:

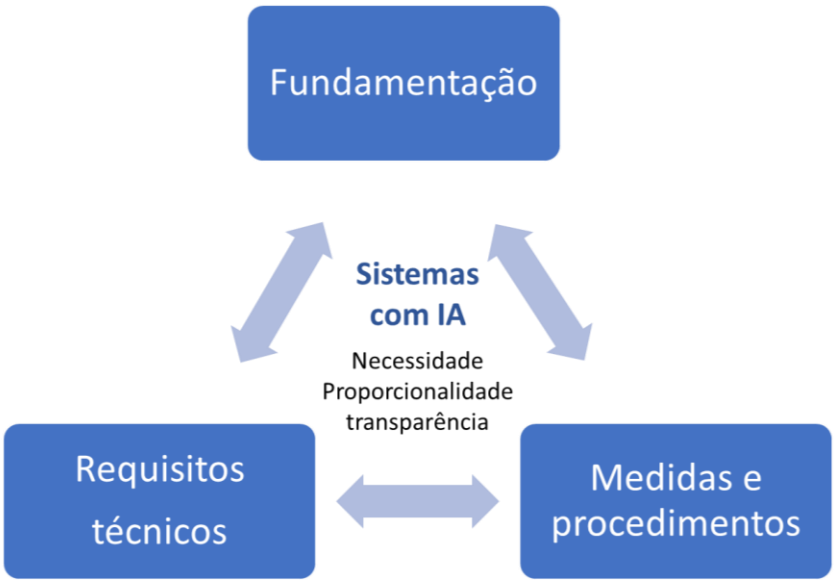

Figura 2 – Domínios da implementação de um sistema de videovigilância policial com IA
Fonte: Lei n.º 59/2019, de 08 de agosto, e Lei n.º 95/2021, de 29 de dezembro.

As mais-valias e potencialidades anteriormente elencadas concorrem para o domínio da Fundamentação, no processo de implementação, sendo relevantes para reforçar a necessidade e o valor acrescido para as FS e para os resultados almejados, no pressuposto do alinhamento com as outras duas dimensões e de forma proporcional às ameaças aos bens jurídicos a salvaguardar.

Conjugando a análise ao ordenamento jurídico com a análise às entrevistas realizadas, aos níveis político, institucional e técnico, reúnem-se boas práticas que se tornam relevantes para a implementação de sistemas de videovigilância policial com IA, as quais concorrem para cada um dos três domínios do processo.

Assim, no concernente à Fundamentação, tornando-se preponderante estabelecer a necessidade e a proporcionalidade, mas também a fiabilidade e a transparência sobre a utilização do sistema com IA, resultam as seguintes boas práticas, identificadas em Quadro 6:

Quadro 6 – Boas práticas para a Fundamentação, no pedido para implementação de sistemas de videovigilância policial em espaços públicos com IA

	Boas práticas	Finalidades/Especificação	Fontes
DA FUNDAMENTAÇÃO	Demonstração da necessidade e proporcionalidade da aplicação de IA	– Demonstração da *imprescindibilidade*, à luz dos fins a que se destina o sistema, e da *proporcionalidade*, através da identificação concreta dos problemas, por exemplo, índices de criminalidade na área de incidência, e o impacto da utilização do sistema com IA nos resultados, com relação entre benefícios e prejuízos, em cumprimento da legislação); – *Transparência* na utilização dos dados, cumprindo a legislação (o sistema de IA não poderá tratar dados que não sejam autorizados); – Utilização da IA para garantia da proteção dos DLG dos cidadãos, em especial a proteção de dados pessoais, em sistema auditado, em cumprimento da legislação.	- Nível político (SEAAI e CNPD) - Nível institucional (MH, GNR)
	Especificação dos critérios, circunstâncias e limites para a utilização de IA	– Estabelecimento das *condições objetivas de utilização*, designadamente, áreas de incidência da captação dos dados e a duração, e os fatores/situações que justificam o recurso ao algoritmo de análise de imagens, incluindo os que devem estar na base da seleção de pessoas e/ou veículos para rastreamento, como por exemplo, no âmbito da investigação criminal, a pesquisa de determinados elementos com características definidas, num local e tempo específico (definição do *conceito de utilização*, de acordo com os parâmetros legais); – Autoria prévia ao sistema, pela CNPD, para assegurar transparência e fiabilidade.	- Nível político (SEAAI e CNPD) - Nível institucional (GNR, GN)
	Avaliação de impacto e demonstração da segurança e fiabilidade do sistema com aplicação de IA	– Levantamento do *impacto e riscos* sobre os DLG e definição de medidas mitigadoras, para salvaguarda da proteção de dados pessoais, demonstrando, nomeadamente, dados que permitam concluir que os resultados apresentados pelo sistema, sobre os quais as FS e o sistema judicial decidirão sobre cidadãos visados, não são discriminatórios e contrários aos princípios constitucionais; – Demonstração da estrutura de cibersegurança; – Manutenção do foco na demonstração da transparência e proporcionalidade do recurso à utilização de IA.	- Nível político (SEAAI e CNPD) - Nível institucional (GNR, GC, GN, AC MH) - Nível técnico
	Demonstração da permanente auditabilidade do sistema	Garantia da *segurança e fiabilidade*, e em especial os registos das operações de tratamento dos dados pessoais, por entidades certificadas.	- Nível político (SEAAI e CNPD) - Nível institucional (GNR, GC, GN, AC MH) - Nível técnico
	Inclusão dos termos do contrato com a Empresa responsável pela instalação, manutenção e substituição dos equipamentos	– Especificação das *funcionalidades* do sistema para a analítica de vídeo, com demonstração do cumprimento dos normativos legais, como forma de reforçar a transparência e a fiabilidade do sistema; – Garantia da *utilização exclusiva* do sistema pela FS, em matéria do seu domínio e controlo, para salvaguarda da segurança e da fiabilidade.	- Nível político (CNPD) - Nível institucional (GNR) - Nível técnico

Fonte: Entrevistas níveis político, institucional e técnico (2022).

Relativamente aos Requisitos Técnicos, conforme sustentado pelos níveis político, institucional e técnico, é fundamental a sua definição, como forma de garantir que o sistema, com IA, funciona da forma estritamente autorizada e com as funcionalidades previstas, para salvaguardar a segurança e a transparência, na sua utilização. As boas práticas, nesta dimensão, encontram-se vertidas em Quadro 7:

Quadro 7 – Boas práticas para os Requisitos Técnicos, no pedido para implementação de sistemas de videovigilância policial em espaços públicos com IA

	Boas práticas	Finalidades/Especificação	Fontes
DOS REQUISITOS TÉCNICOS	Identificação da forma de recolha, transmissão e conservação das imagens	Em especial as *características* que permitam: – *Utilização exclusiva* do sistema pela FS (integral de um fabricante, para facilitar as definições de segurança e a responsabilização); – Acesso ao sistema de visualização e/ou extração de imagens mediante *perfis de acesso* e somente com sistema de *dupla autenticação* (senha e QR *code*, a título de exemplo), de forma *presencial*; – Aplicação de *software de filtros de ocultação* em locais privados e respetivos acessos (portas e janelas), que impeça a captação de imagem e de som – neste caso, devem ser assinaladas as zonas a filtrar nas áreas de incidência, assim como identificadas as câmaras e respetivos ângulos de visão; – *Encriptação das imagens*, desde a captação (na câmara) até à visualização destas, ou seja, em todo o canal de comunicação captação-gravação-gestão; – Arquivamento dos dados com *encriptação fotograma a fotograma*, compondo *imagens sem descrição e sem vínculo bidirecional*, apenas passível de ser atribuído mediante ação do agente operador e/ou supervisor do sistema, facilitando a gestão dos dados não vinculativa e promovendo a sua inviolabilidade; – *Gravação* dos dados registados somente *nos meios físicos* especificamente *definidos e autorizados*; – Inscrição, nos dados captados, de forma inequívoca, da data, hora, local e equipamento de captura; – Aplicação de *mecanismos de anonimização* para as imagens de vídeo, para impossibilidade de criação de perfis ou discriminação de pessoas; – *Conservação dos dados* captados em registo codificado, pelo prazo máximo de 30 dias, contados a partir da data de captação; – Mecanismos de segurança e proteção da rede e sistemas utilizados, como dos dados captados, a fim de não serem comprometidos por qualquer ciberameaça (estrutura de cibersegurança).	- Nível político (CNPD) - Nível institucional (GNR, GC, GN, AC, MH) - Nível técnico
	Utilização de base de dados própria e encriptada	Garantia da segurança e fiabilidade do sistema.	- Nível político (CNPD) - Nível institucional (GNR) - Nível técnico
	Uso de sistema operativo baseado em Linux	Facilitação da inviolabilidade dos dados (segurança).	- Nível técnico

Fonte: Entrevistas aplicadas, níveis político, institucional e técnico, 2022.

Quanto às Medidas e Procedimentos para mitigar os riscos e a assegurar a proteção dos dados pessoais e a segurança do sistema, bem como a transparência na sua utilização, são elencadas as boas práticas em Quadro 8:

Quadro 8 – Boas práticas para Medidas e Procedimentos, no pedido para implementação de sistemas de videovigilância policial em espaços públicos com IA

	Boas práticas	Finalidades/Especificação	Fontes
DAS MEDIDAS E PROCEDIMENTOS PARA PROTEÇÃO DOS DADOS	Definição de regras e critérios para utilização do sistema com aplicação de IA	– Definição do conjunto de procedimentos para os operadores do sistema; – Definição de um responsável, contemplando, nomeadamente, a preservação de imagens extraídas, no âmbito da investigação criminal, incluindo como são excecionadas da rotatividade de 30 dias do arquivo do sistema, bem como a sua eliminação, após a conclusão do processo-crime.	- Nível político (SEAAI e CNPD) - Nível institucional (GNR, MH, AC)
	Segregação física e lógica das redes de videovigilância das outras redes	Aplicação de protocolo HTTPS, para garantia da segurança do sistema.	- Nível político (CNPD) - Nível institucional (GNR) - Nível técnico
	Segurança física do sistema	– Inclusão de sistema anti-tampering nos armários de comunicações, com alertas, além da existência de plataformas de *software* que permitam acompanhar o estado dos equipamentos que interagem, como as câmaras, designadamente o Site Health; – Localização dos armários de comunicações em pontos que dificultem o acesso, nos locais públicos.	- Nível político (CNPD) - Nível institucional (GNR)
	Auditorias ao sistema	– Realização com caráter regular e programado, mas, também, inopinadamente; – Ao funcionamento do sistema, à estrutura de cibersegurança, ao registo das operações de tratamento dos dados e ao cumprimento dos procedimentos estabelecidos, relativamente à captação, acesso e tratamento - essencial registos cronológicos com detalhe do operador e o que fez; – Ao registo de todas as ações efetuadas por um utilizador, incluindo tentativas de acesso, assim como a obrigação de garantia da sua integridade, através de assinatura e TimeStamp.	- Nível político (SEAAI e CNPD) - Nível institucional (GNR) -Nível técnico
	Contratação da instalação, manutenção e substituição dos equipamentos	A uma única Empresa, com absoluta garantia que a FS mantém em permanência o domínio e controlo da gestão do sistema e do tratamento dos dados.	- Nível político (CNPD) - Nível institucional (GNR) - Nível técnico
	sistema de cópias de segurança dos dados	– Garantia da disponibilidade dos dados, no prazo dos 30 dias, em caso de eliminação acidental, para além das condições previstas para a sua recuperação, em caso de avarias no armazenamento; – Quantificação de dois servidores, em cenário de failover, com a arquitetura de partilha da unidade dedicada a armazenamento de dados, assegurando, assim, a continuidade do sistema, em caso de falha no servidor ativo.	- Nível político (CNPD) - Nível institucional (GNR)
	Formação	Formação e credenciação específica aos operadores e gestores do sistema.	- Nível político (CNPD) - Nível institucional (GNR) - Nível técnico

Fonte: Entrevistas aplicadas, níveis político, institucional e técnico, 2022.

6. Conclusões

A globalização e a evolução tecnológica trazem associados desafios e ameaças que requerem a conjugação de esforços, no desiderato de promover a Segurança, com base numa política assente nos valores comuns europeus e com primazia ao Estado de Direito e à salvaguarda dos Direitos Fundamentais.

As ferramentas tecnológicas, em especial as que aplicam IA, têm dado provas de potenciar a eficácia e a eficiência nos diversos setores da sociedade, em que se inclui o da Segurança.

Neste contexto, considerando a atuação das FS, e, em concreto, os recursos tecnológicos que utilizam, têm assumido preponderância os sistemas de videovigilância policial em espaços públicos, em que a aplicação de IA, apesar de conferir reconhecidas mais-valias, aporta, igualmente, questões relacionadas com a salvaguarda dos DLG, sobretudo a proteção de dados pessoais, as quais têm que ser dirimidas para a implementação esta tecnologia.

Na senda, considerando o tema do presente trabalho, "O impacto da tecnologia no policiamento", e sendo a IA o desenvolvimento tecnológico com capacidade para alterar o paradigma atual do policiamento, mas que apresenta resistência e dificuldades de implementação, considerou-se pertinente que a investigação devesse integrar como objeto de estudo a IA nos sistemas de videovigilância policial.

Para a investigação, seguiu-se o raciocínio dedutivo, adotando um desenho de pesquisa por estudo de caso e uma estratégia qualitativa, baseada em análise documental e na realização de entrevistas semiestruturadas, numa perspetiva de *benchmarking*. O percurso metodológico foi constituído por duas fases: na primeira efetuou-se a pesquisa de informação e revisão literária, para estabelecer a base concetual e os objetivos e questões a responder, tendo tido como corolário a matriz de análise do presente estudo, que foi o suporte da investigação, e, na segunda, foi seguido o percurso metodológico definido e promovida a análise, tendo sido respondida a QC "Que boas práticas podem ser adotadas para aplicar IA em sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor?", e alcançado o OG, de propor boas práticas para a aplicação de IA nos sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor.

A Estratégia da UE para a Segurança espelha a premência de reforçar a proteção física dos espaços públicos, com sistemas de deteção adequados, mas com salvaguarda dos direitos e liberdades dos cidadãos, nomeadamente no que se refere à proteção dos dados pessoais e ao respeito pela vida privada e familiar.

O desenvolvimento de IA é uma realidade e tanto tem o potencial de trazer benefícios ao quotidiano da vida em sociedade como o de fazer perigar a Segurança e os direitos fundamentais, consoante a utilização que seja feita desta tecnologia. Neste sentido, tal utilização (de IA) terá que ser regulada, sendo esse o desiderato da UE, que a pretende promover, de forma compatível com os direitos fundamentais, através de sistemas seguros e fiáveis, para benefício comum.

O CE, a este respeito, publicou o Livro Branco da IA, que visa tornar esta tecnologia fiável e segura. No alinhamento, encontra-se a ser discutido, para aprovação, um regulamento para o estabelecimento das regras de desenvolvimento e utilização de IA na UE, abordando os riscos associados e produzindo conclusões que reforçam a importância de responder a desafios como a opacidade, a complexidade, os preconceitos e um determinado grau de imprevisibilidade e autonomia parcial destes sistemas, com vista a garantir a sua compatibilidade com os direitos fundamentais e a aplicação das normas jurídicas.

Sendo indubitável que a utilização dos novos instrumentos tecnológicos, com aplicação de IA, pelas FS, potencia a eficiência (dos recursos) e a eficácia (dos resultados), tanto na prevenção e na luta contra a criminalidade, como na garantia dos direitos fundamentais, devem, neste domínio, ser salvaguardados elevados padrões de conformidade, assegurando uma proteção eficaz dos direitos dos cidadãos.

A aplicação de IA nos sistemas de videovigilância policial é, per si, um contributo para a salvaguarda dos direitos fundamentais dos cidadãos, na medida em que tem por fim garantir a Segurança. Esta última constitui-se uma tarefa fundamental do Estado, devendo observar os princípios constitucionais, como o da proporcionalidade e o da privacidade, pelo que deverá ter em conta o equilíbrio entre o bem jurídico a preservar e o impacto dos meios necessários, que devem ser empregues na medida do estritamente necessário e por forma a não causar constrangimentos que possam ser evitáveis.

À luz do referido, no decorrer da evolução tecnológica e dos impactos da crescente globalização, foram introduzidos mecanismos com vista à proteção da esfera individual dos cidadãos, nomeadamente o RGPD, e, também, neste contexto, a Diretiva (UE) 2016/680, relativa ao tratamento de dados pessoais pelas autoridades competentes para efeitos de

prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, que assume preponderância sobre a videovigilância policial.

No cômputo nacional, transpondo o quadro jurídico comunitário, encontra-se em vigor a Lei n.º 95/2021, de 29 de dezembro, que regula a utilização e o acesso a sistemas de videovigilância, para captação, gravação e tratamento de imagem e som, assim como as Leis n.º 58/2019 e n.º 59/2019, ambas de 8 de agosto, e, ainda, as Portarias n.º 372/2012 e n.º 373/2012, ambas de 16 de novembro, que regulamentam a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, designadamente no que diz respeito aos requisitos técnicos e à simbologia prevista.

Em matéria de controlo e fiscalização, ao nível europeu, existe o CEPD, composto por representantes das autoridades nacionais para a proteção de dados dos Estados Membros da UE e pela Autoridade Europeia de Proteção de Dados. A nível nacional, a autoridade de controlo é a CNPD, sendo responsável pela fiscalização do cumprimento do RGPD e dos normativos vigentes, conforme referido.

Respondeu-se, assim, à QD1, quanto ao ordenamento jurídico aplicável à videovigilância policial em espaços públicos, no contexto europeu, e a sua transposição nacional.

Da análise efetuada, conclui-se que os normativos jurídicos não proíbem a utilização de IA, admitindo que o tratamento de dados tenha subjacente um sistema de gestão analítica, por aplicação de critérios técnicos, de acordo com os fins a que se destinam os sistemas, os quais devem ser previamente definidos e autorizados, no que se refere à aplicação de IA, incluindo a especificação concreta dos termos inerentes ao recurso a esta tecnologia.

Neste domínio, está prevista a publicação da regulamentação à legislação vigente, que trará orientações específicas sobre os requisitos técnicos que a solução analítica de dados deve observar. Neste particular, de salientar que, até ao momento, cada FS faz a instrução do projeto que submete à aprovação da Tutela, em observância do ordenamento jurídico e propondo medidas específicas para mitigar os riscos identificados, à luz do sistema que pretende implementar e da avaliação do impacto deste nos DLG dos cidadãos, mas sem ter, atualmente, *à priori*, a definição dos critérios técnicos que a analítica de vídeo pode contemplar, ou o acesso a eventuais boas práticas para a sua utilização.

Considera-se, desta forma, reunida a resposta à QD2, concluindo-se que a GNR pode, numa perspetiva legal e técnica, em cumprimento do ordenamento jurídico em vigor, aplicar

IA nos sistemas de videovigilância em espaços públicos, não obstante essa aplicação carecer de um parecer favorável da CNPD.

Para aprofundar o estudo sobre a aplicabilidade de IA nos sistemas de videovigilância policial, em cumprimento dos normativos jurídicos e a forma de garantir a segurança e a fiabilidade, no que concerne à proteção dos dados e dos DLG dos cidadãos, tornou-se essencial complementar a análise documental, com informação específica de três níveis: Político, no domínio da aprovação dos projetos de videovigilância policial e da regulamentação dos critérios técnicos para o recurso a analítica de vídeo com aplicação de IA; Institucional, sobre a implementação dos sistemas, pelas FS, analisando-se a aplicação de IA, concretamente pela GNR, GC, a GN, a AC e a MH, numa ótica de *benchmarking*, assim como a sua perspetiva relativamente à temática; e Técnico, no que respeita à instalação, manutenção e substituição dos equipamentos de videovigilância (com vista a complementar a análise relacionada com os requisitos técnicos).

A analítica de vídeo tem diversas possibilidades de aplicação, incluindo a utilização de IA, com base em algoritmos, mais ou menos evolutivos e com maior ou menor autonomia, que podem funcionar de formas diferentes, dependendo do que se pretende analisar. Esta solução possibilita analisar elevados volumes de imagens, correlacionar dados e situações que, individualmente, não levantariam suspeitas, criando um tipo de ação ou alerta, para que o operador do sistema possa avaliar e decidir, trazendo, assim, um potencial inigualável para as operações de segurança.

Considerando o impacto que a analítica de vídeo tem, não só na prevenção, como na investigação, torna-se preponderante que os sistemas tenham capacidade de filtrar pesquisas com base em *metadados*, permitindo consultas específicas, sobre um objeto com determinadas características, num período definido, assim como a deteção de padrões e tendências, também relevante no planeamento de operações e alocação de recursos.

Estas ferramentas consideram-se muito relevantes para a prevenção e investigação de criminalidade grave e organizada, como o terrorismo, ou, ainda, no contexto de pessoas desaparecidas ou vítimas de fenómenos criminais como o tráfico de seres humanos. Poderão, de facto, trazer uma vantagem preciosa à atuação policial, que fará a diferença para salvar vidas humanas, em casos específicos, na medida em que os sistemas, funcionando como um radar preditivo, possibilitam detetar padrões suspeitos que constituam ameaças concretas, e, assim, agir em antecipação, ao invés de reagir.

Da análise, foi possível concluir que todas as cinco FS congéneres, sendo responsáveis pela proteção de pessoas e bens nas suas áreas de responsabilidade, realizam policiamento orientado pelas informações policiais, assim como utilizam sistemas informáticos, no quadro da recolha e análise de dados, elaboram relatórios de informações e mapas de risco da criminalidade, assim como utilizam sistemas informáticos de informações criminais, interoperáveis com outras Entidades no setor da Segurança, ao nível nacional, para partilha de informação.

Na senda, também todas consideram que estas ações de policiamento promovem a rentabilização dos recursos policiais e referem que a implementação de videovigilância policial em espaços públicos pode contribuir para a capacidade preditiva e que a aplicação de IA nos sistemas aduz mais valias, mas, também, a necessidade de medidas de segurança e mecanismos para assegurar a proteção dos dados pessoais e a conformidade do seu tratamento, decorrente do ordenamento jurídico vigente.

Das FS congéneres europeias, apenas a italiana confirmou aplicar IA nos seus sistemas de videovigilância em espaços públicos. Não obstante, tendo-se reunido a perspetiva de todas, sobre esta questão, foi possível constatar que desenvolvem ferramentas de IA para facilitar a sua atividade diária, em diversas áreas, com especial ênfase à congénere holandesa que está a preparar a aplicação de IA neste domínio da videovigilância policial, estando a trabalhar na inovação tecnológica por experimentação, em estreita colaboração com centros de estudo, universidades e agências governamentais, nomeadamente no desenvolvimento de Visão Computacional baseada em IA, com a designada Deteção Comportamental (*behavior detection*) para detetar automaticamente comportamentos humanos indesejados ou anormais, em filmagens de câmaras.

Na sequência da resposta à QD3, em que se analisou a aplicação de IA pelas FS congéneres e se obteve a perspetiva destas sobre a temática, foi possível reforçar algumas questões a salvaguardar, designadamente a importância de manter a decisão humana (a par da utilização de sistemas automáticos), a necessidade de manter um permanente acompanhamento da evolução tecnológica, da partilha de informação entre FS, da observação dos normativos legais (especialmente restrições decorrentes), da validação prévia por operadores humanos dos resultados dos algoritmos, do desenvolvimento de métodos de anonimização para as imagens de vídeo e do desenvolvimento de um Manifesto Ético relativamente à IA, com as diretrizes éticas seguidas e especificadas as possíveis

questões neste domínio, com base nos regulamentos europeus e num trabalho que envolva colaboração com juristas experientes na área da análise de dados para fins policiais.

Como corolário do trabalho de investigação, foi possível responder à QC definida, que cumpre o OG, propondo um conjunto de boas práticas para a aplicação de IA em sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor, as quais se encontram explanadas no Apêndice G, não se replicando aqui por economia de espaço. As boas práticas propostas incidem, sobretudo, nos elementos a incluir no pedido de autorização para a implementação dos sistemas de videovigilância com aplicação de IA na gestão analítica dos dados, com ênfase na fundamentação, nos requisitos técnicos dos equipamentos e nas medidas e procedimentos para proteção dos dados pessoais e da segurança do sistema, incluindo no domínio da cibersegurança.

Considera-se que a investigação reúne contributos sólidos, úteis e passíveis de serem adotados na GNR, com base num estudo credível e sustentado, numa abordagem inovadora e que se considera premente, face ao Estado da Arte. Trata-se de um trabalho original, do qual resultam propostas concretas, que se considera acrescentarem valor ao conhecimento sobre a temática, sendo suscetíveis de melhorar o serviço operacional da Guarda e, por inerência, trazer benefícios à população que serve.

Como estudos futuros, sugere-se investigar o desenvolvimento de aplicações de IA que possam ser implementadas nos sistemas de videovigilância, em cumprimento do ordenamento jurídico em vigor, e à luz dos fins a que se destinam, por forma a potenciar a função policial e os resultados desta.

Como limitação ao desenvolvimento do trabalho, aponta-se o facto de a CNPD não ter concedido entrevista, o que não permitiu aprofundar algumas questões relevantes, designadamente ao nível dos critérios de aplicação de IA.

Por fim, apresenta-se a recomendação de que, antes da publicação da regulamentação à Lei nº 95/2021, de 29 de dezembro, sejam analisadas as boas práticas resultantes desta investigação, podendo servir como base, de necessidades práticas, na perspetiva da aplicação da matéria que será regulamentada, durante a sua elaboração.

Referências bibliográficas

Associação FIEP (2022a). *Forças que integram a FIEP*. [Página *online*]. Retirado de http://www.fiep.org/member-forces/.

Associação FIEP (2022b). *Relatório Técnico da Reunião da Comissão de Logística e Novas Tecnologias*. Lisboa.

Bryman, A. (2012). *Social research methods* (Fourth edi). Oxford University Press.

Caetano, M. (2008). *Manual de Direito Administrativo*. (Vol. II. 10.ª Ed.). Coimbra: Almedina.

Comissão Europeia (2016). Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril. *Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados*. Jornal Oficial da União Europeia, L 119/89. Bruxelas: UE.

Comissão Europeia (2020a). *Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a Estratégia da União Europeia para a União da Segurança*. Bruxelas: EU.

Comissão Europeia (2020b). *Livro branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança* [versão PDF]. Retirado de https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_pt.pdf

Comissão Europeia (2021). *Proposta de regulação europeia 2021/006 (COD). Que estabelece regras harmonizadas em matéria de Inteligência Artificial (Regulamento Inteligência Artificial) e altera determinados atos legislativos da união*. [versão PDF]. Retirado de https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN.

Comissão Europeia (2022). *O que significa a proteção de dados «desde a conceção» e «por defeito»?*. [Página *online*]. Retirado de https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_pt.

Comissão Nacional de Proteção de Dados (2021). *Parecer/2021/125 sobre o pedido de autorização para utilização de um sistema de videovigilância nas zonas da Oura e Baixa de Albufeira, submetido pela Guarda Nacional Republicana*. Lisboa.

Comissão Nacional de Proteção de Dados (2022). [Página *online*]. Retirado de https://www.cnpd.pt.

Computer World (2022). *O futuro da análise de vídeo com Inteligência Artificial*. [Página *online*]. Retirado de https://www.computerworld.com.pt/2022/03/14/o-futuro-da-analise-de-video-com-inteligencia-artificial/.

Guarda Nacional Republicana (2020a). *Estratégia da Guarda 2025, uma estratégia centrada nas pessoas*. Lisboa.

Guarda Nacional Republicana (2020b). *Plano Operacional Setorial 2025 da GNR*. Lisboa.

IUM (2020). *NEP/INV - 001 - Trabalhos de Investigação*. Lisboa. Instituto Universitário Militar.

IUM (2020). *NEP/INV - 003 - Regras de Apresentação e de Referenciação para os Trabalhos Escritos a Realizar no IESM*. Lisboa. Instituto Universitário Militar.

Fernandes, F. (2020). *Inteligência Artificial, Segurança e Direitos* (Dissertação de Mestrado em Segurança da Informação e Direito do Ciberespaço). Instituto Superior Técnico [IST]. Lisboa: IST.

Freixo, M. J. V. (2012). *Metodologia Científica, fundamentos métodos e técnicas* (4ª Edição). Lisboa: Instituto Piaget.

Moleirinho, P. (2018). *A importância dos modelos preditivos na área da segurança. Entre riscos e equilíbrios instáveis*. Em: Fronteira do Caos Editores Lda. e Autores, Modelos Preditivos e Segurança Pública (pp. 99-130). Porto.

Moleirinho, P. (2021). *Aplicação da Inteligência Artificial ao Serviço da Função Policial*. Lisboa. Instituto Universitário Militar.

Morgan, F., Boudreaux, B., Lohn, A., Ashby, M., Curriden, C., Klima, K., Grossman, D. (2020). *Military Applications of Artificial Intelligence - Ethical Concerns in an Uncertain World*. California: Rand Corporation. Retirado de https://www.rand.org/pubs/research_reports/RR3139-1.html.

Gouveia, J. B. (2018). *Direito da Segurança, Cidadania, Soberania e Cosmopolitismo*. Coimbra: Edições Almedina, S.A.

Quivy, R. & Van Campenhoudt, L. (2008). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva.

Lee, K. (2018). *As Superpotências da Inteligência Artificial – A China, Silicon Valley e a Nova Ordem Mundial*. Lisboa: Relógio D´Água.

Lei n.º 1/1976, de 10 de abril (1976). *Constituição da República Portuguesa*. Diário da

República n.º 86/1976, Série I. Lisboa: Assembleia da República.

Lei n.º 1/2005, de 12 de agosto (2005). *Sétima revisão constitucional*. Diário da República, I Série, 155, 4642. Lisboa: Assembleia da República.

Lei n.º 1/2005, de 10 de janeiro (2005). *Regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum*. Diário da República, I Série, 205. Lisboa: Assembleia da República.

Lei n.º 53/2008, de 29 de agosto (2020). *Lei de Segurança Interna*. Diário da República, 1.ª Série, 167, 6135-6141. Lisboa: Assembleia da República.

Lei n.º 9/2012, de 23 de fevereiro (2012). *Procede à terceira alteração à Lei n.º 1/2005, de 10 de janeiro, que regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum*. Diário da República, I Série, 39, 868. Lisboa: Assembleia da República.

Lei n.º 58/2019, de 8 de agosto (2019). *Lei de proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Diário da República n.º 151, 1.ª série. Lisboa: Assembleia da República.

Lei n.º 59/2019, de 8 de agosto (2019). *Lei de tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais*. Diário da República n.º 151, 1.ª série. Lisboa: Assembleia da República.

Lei n.º 95/2021, de 29 de dezembro (2021). *Regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som, revogando a Lei n.º 1/2005, de 10 de janeiro*. Diário da República n.º 251, 1.ª série. Lisboa: Assembleia da República.

Lourenço, N., Costa, A. (2018). *Estratégia de Segurança Nacional, Portugal Horizonte 2030*. Coimbra: Edições Almedina, S.A.

OSCE. (2017). *The OSCE Project on Intelligence-Led Policing From Reactive to Proactive Policing*. Vienna.

Parlamento Europeu. (2021). *O que é a Inteligência Artificial e como funciona?*. Retirado de https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona

Pereira, L. (2017). *Políticas de Segurança e a videovigilância urbana - o caso da Amadora* (IV Curso de Direção e Estratégia Policial). Instituto Superior de Ciências Policiais e

Segurança Interna. Lisboa.

Portaria n.º 372/2012, de 16 de novembro (2012). *Fixa os requisitos técnicos mínimos das câmaras fixas e portáteis nos termos do n.º 7 do artigo 5.º e do n.º 1 do artigo 6.º da Lei n.º 1/2005, de 10 de janeiro, alterada pela Lei n.º 39 -A/2005, de 29 de julho, pela Lei n.º 53 -A/2006, de 29 de dezembro, e pela Lei n.º 9/2012, de 23 de fevereiro, que a republica*. Diário da República, I Série, 222. Lisboa: Assembleia da República.

Portaria n.º 373/2012, de 16 de novembro (2012). *Regula a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum, com as alterações introduzidas pela Lei n.º 39 -A/2005, de 29 de julho, pela Lei n.º 53 -A/2006, de 29 de dezembro, e pela Lei n.º 9/2012, de 23 de fevereiro, que a republicou, estabelece no artigo 4.º a obrigatoriedade de afixação, nos locais objeto de vigilância com recurso a câmaras fixas, de informação sobre a existência e localização das câmaras de vídeo, a finalidade da captação de imagens e sons e o responsável pelo tratamento dos dados recolhidos*. Diário da República, I Série, 222. Lisboa: Assembleia da República.

Raposo, J, Gouveia, J. & F. P. Coutinho (2013). Polícia. Em *Enciclopédia da Constituição Portuguesa* (pp. 282–84). Lisboa: Quid Juris.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril (2016). *Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)*. Jornal Oficial da União Europeia, L 119/1. Bruxelas: UE.

Santos, L. A. B., & Lima, J. M. M. (Coord. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação*. (2.ª Ed., revista e atualizada). Cadernos do IUM, 8. Lisboa: Instituto Universitário Militar.

Sarmento, M. (2013). *Metodologia Científica para a elaboração e apresentação de teses*. Lisboa: UAL.

Silva Costa, I. (2021). *A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas*. Revista Electrónica de Direito, 24(1), 33–82.

Sistema de Segurança Interna (2012). *Relatório Anual de Segurança Interna* 2011. Lisboa.

Secretaria Geral do Ministério da Administração Interna (2020). *Dossier Temático Videovigilância*. Lisboa: SGMAI.

Secretaria Geral da Presidência do Conselho de Ministros (2022). *Regulamento Geral de*

Proteção de Dados. [Página *online*]. Retirado de https://www.sg.pcm.gov.pt/sobre-nos/regulamento-geral-de-prote%C3%A7%C3%A3o-de-dados.aspx.

Security Magazine (2021). *Uma Nova Era para a Analítica de Vídeo*. [Página *online*]. Retirado de https://www.securitymagazine.pt/2021/12/08/uma-nova-era-para-a-analitica-de-video/.

Segurança Eletrónica (2022). *O que é Vídeo Analítico e como ele funciona*. [Página *online*]. Retirado de https://revistasegurancaeletronica.com.br/o-que-e-video-analitico-e-como-ele-funciona/.

Strom, K. (2017). *Research on the Impact of Technology on Policing Strategy in the 21st Century, Final Report*. National Criminal Justice Reference Service, 153.

TekSapo (2022). *Parlamento Europeu exige salvaguardas no uso de sistemas de videovigilância com IA pela polícia*. [Página *online*]. Retirado de https://tek.sapo.pt/noticias/computadores/artigos/parlamento-europeu-exige-salvaguardas-no-uso-de-sistemas-de-videovigilancia-com-ia-pela-policia.

União Europeia. (2012). *Carta dos Direitos Fundamentais da União Europeia*. Bruxelas: Jornal Oficial da União Europeia, C 326/391

União Europeia. (2016). *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados* e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Parlamento Europeu.

Valente, M. (2014). *Teoria Geral do Direito Policial*. Lisboa: Almedina

Apêndice A – Modelo de análise

Quadro 9 – Modelo de análise

Tema: O impacto da tecnologia no policiamento.	
Questão Central: Que boas práticas podem ser adotadas para aplicar IA em sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor?	
Objeto de estudo: IA na videovigilância policial.	
Objetivo Geral: Propor boas práticas para a aplicação de IA nos sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico em vigor.	
OE1: Analisar o ordenamento jurídico aplicável à videovigilância policial em espaços públicos, no contexto europeu e a sua transposição nacional.	**Cap 3**
QD1: Qual o ordenamento jurídico aplicável à videovigilância policial em espaços públicos, no contexto europeu, e qual a sua transposição nacional?	
OE2: Analisar a aplicação de IA nos sistemas de videovigilância da GNR em espaços públicos, à luz do ordenamento jurídico em vigor.	**Cap 4**
QD2: Pode a GNR aplicar IA nos sistemas de videovigilância em espaços públicos, em cumprimento do ordenamento jurídico em vigor?	
OE3: Analisar a aplicação de IA nos sistemas de videovigilância em espaços públicos pelas FS congéneres europeias, à luz do ordenamento jurídico em vigor.	**Cap 4**
QD3: Aplicam as FS congéneres europeias IA nos seus sistemas de videovigilância em espaços públicos, em cumprimento do ordenamento jurídico em vigor?	
Métodos e procedimentos de pesquisa e recolha de informação	
Análise documental e Entrevistas semiestruturadas	

Conceitos	Dimensões	Variáveis	Indicadores
Policiamento	Policiamento Preditivo	Recolha de informações policiais	Técnicas e procedimentos de recolha de informações
			Utilização de sistemas informáticos
		Análise de dados	Produção de relatórios de informações
			Elaboração de mapa de risco criminal na área de responsabilidade
			Utilização de sistemas informáticos interoperáveis com outras entidades
		Ações de policiamento orientado pela análise de informações	Realização de ações de policiamento orientado pela análise de informações policiais
			Diminuição da taxa de criminalidade nos locais de realização do policiamento
			Rentabilização dos recursos policiais
Videovigilância	Videovigilância Policial (locais públicos)	Capacidade de tratamento e análise de dados	Características técnicas dos equipamentos, incluindo especificações para proteção dos DLG, conforme ordenamento jurídico em vigor
			Aplicação de IA para tratamento e análise de dados
		Maximização da atuação policial	Conexão a bases de dados de informações criminais
			Aumento da capacidade preditiva e da eficácia da atuação policial
Inteligência Artificial	Analítica de vídeo	Capacidade de identificar perfis de suspeitos	Utilização de aplicações de identificação de perfis suspeitos
		Capacidade de detetar e analisar movimentos/padrões	Utilização de aplicações de análise de movimentos e deteção de padrões suspeitos na vigilância de espaços públicos
		Capacidade de controlo de tráfego	Utilização de aplicações de controlo de tráfego
Proteção de Dados	RGPD	Proteção dos DLG dos Cidadãos	Avaliação do impacto das operações de tratamento de dados, nos DLG
			Garantias, medidas de segurança e mecanismos para assegurar a proteção dos DLG
			Entidade responsável pelo exercício dos direitos de acesso e retificação dos dados
		Cumprimento da regulamentação europeia	Medidas gerais decorrentes da transposição nacional da regulamentação europeia
			Procedimentos internos para salvaguarda do cumprimento da regulamentação europeia, na aplicação de IA em videovigilância policial

Apêndice B – Glossário de conceitos complementares

Algoritmo

Conforme explana Moleirinho, citando Domingos (2017), "um algoritmo é uma sequência de instruções que diz a um computador o que fazer […]. Os algoritmos evolutivos conseguem […] unir pontos entre acontecimentos que, individualmente, parecem inofensivos, mas que em conjunto constituem um padrão ameaçador" (2021, p. Apd A-4). Estabelece-se, neste domínio, citando Domingos (2017), que a Aprendizagem de Máquina (ou automática) funciona como um radar preditivo que possibilita antecipar e evitar as manobras do adversário, ao invés de reagir, sendo que a Aprendizagem Profunda, ramo mais recente da IA, utiliza algoritmos baseados em dados gerados pelas interações de múltiplas camadas de Aprendizagem de Máquina (Moleirinho, 2021, p. Apd A-4).

A conjugação entre a recolha de imagens e a capacidade de as analisar e criar um tipo de ação ou alerta, com base no resultado, exponencia as operações de segurança, no que se refere à eficácia e à eficiência dos recursos (Security Magazine, 2021).

Metadados

Podem ser definidos como dados sobre outros dados, descrevendo, na vigilância por vídeo, a informação sobre o que está a ser visionado, como por exemplo a classificação dos objetos, incluindo veículos e pessoas, assim como os atributos associados a esses objetos, como por exemplo, as cores, a direção do movimento, entre outros (Security Magazine, 2021).

Alonso refere que "num contexto onde o número de câmaras aumentou exponencialmente, as gravações de vídeo geram enormes arquivos de imagens, os recursos humanos são escassos e dispendiosos, e como tal a automatização do processo é crucial para a otimização da segurança" (Computerworld, 2022).

Salienta, ainda, que a primeira utilização da análise de vídeo, no domínio da segurança, visou a deteção de incidentes e situações de risco, no entanto, com a evolução dos sistemas de videovigilância, o impacto da utilização será maior no âmbito da investigação. Em tal desiderato, torna-se preponderante que os sistemas tenham a capacidade de filtrar pesquisas com base em atributos (tipo, cor, direção, etc.) previamente etiquetados através da analítica, sendo que muitas destas se destinam a fornecer dados, precisamente para facilitar pesquisas ou para construir análises e estatísticas - os designados *metadados.* O mesmo autor conclui que constituem estes os fatores que farão a diferença na exploração de novos sistemas de vídeo utilizando a analítica baseada em Inteligência Artificial. (Computerworld, 2022)

Proteção de Dados,

Estabelecendo o seu significado *desde a conceção* e *por defeito*, em que, de acordo com a Comissão Europeia (CE) e com referência ao Regime Geral de Proteção de Dados (RGPD),

> […] As empresas/organizações são incentivadas a aplicar medidas técnicas e organizativas, nas fases iniciais da conceção das operações de tratamento, de forma a garantir os princípios da privacidade e proteção de dados logo desde o início («proteção de dados desde a conceção»). Por defeito, as empresas/organizações devem garantir que os dados pessoais sejam tratados com a mais elevada proteção da privacidade (por exemplo, apenas os dados necessários devem ser tratados, período de conservação curto, acessibilidade limitada) para que, por defeito, os dados pessoais não sejam disponibilizados a um número indefinido de pessoas - «proteção de dados por defeito» (CE, 2022).

São, na senda, apresentados os seguintes exemplos de Proteção de Dados *desde a conceção* e por *defeito*:

> […] O recurso à pseudonimização (substituição de material pessoalmente identificável por identificadores artificiais) e à cifragem (codificação de mensagens para que apenas as pessoas autorizadas as possam ler). Uma plataforma de redes sociais deve ser incentivada a definir as configurações de perfil dos utilizadores de forma a facilitar o mais possível a privacidade, por exemplo limitando desde o início a acessibilidade do perfil dos utilizadores para que este não seja acessível por defeito a um número indefinido de pessoas (CE, 2022).
>
> Os **dados pessoais** são definidos como
>
> […] informações relativas a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular. (CE, 2016)
>
> O **tratamento** (de dados pessoais), consiste numa
>
> […] operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação

por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição. (CE, 2016)

Vídeo Analítico,
Também designado como *Análise Inteligente de Vídeo*, consiste numa tecnologia com capacidade para proceder à análise de imagens de vídeo, com a finalidade de detetar e identificar eventos e objetos automaticamente (Segurança Eletrónica, 2022). Trata-se de uma solução de IA e *Visão Computacional*, em que as câmaras podem ser equiparadas a "olhos" de um sistema de vídeo analítico, que, por sua vez, será equivalente a um "cérebro", que vai analisar e compreender o que está a ser visualizado, sendo as possibilidades de aplicação inúmeras, desde a simples deteção de elementos específicos até ao rastreamento desses elementos na imagem (Segurança Eletrónica, 2022).
A tecnologia de *Vídeo Analítico* funciona através de um algoritmo treinado para reconhecer imagens específicas e movimentos, podendo funcionar de diversas formas, dependendo do que se pretende analisar, constituindo as principais e mais utilizadas: a deteção de elementos específicos, o cruzamento de Linha Virtual, a ROI – *Region of Interest*, o sentido do movimento, o reconhecimento de comportamentos e a contagem de elementos (Segurança Eletrónica, 2022).

Quadro 10 – Evolução da analítica de vídeo

EVOLUÇÃO DA ANALÍTICA DE VÍDEO	
Primeira Fase	
Fotogramas baseados em *motion*	Analítica com elevados falsos positivos e análise vetorial da captura de imagem inexistente.
Segunda Fase	
Evolução para *advanced motion*	Necessidade de dispor de equipamentos adicionais, para além do gravador de imagem, assim como de *softwares* para processar novamente as imagens, no intuito de encontrar dados que correspondam aos padrões pré-vetorizados, o que gerava, ainda, elevados falsos positivos e elevado dispêndio de tempo nas aplicações, a par do facto de não terem a capacidade para se adaptar num dado grau de probabilidade vetorial.
Terceira Fase	
VideoIQ	Solução do problema (principal) de falsos positivos, isto é, a variação de vetores, dando um determinado grau de probabilidade e confiança, para cada objeto capturado, tendo a analítica "embebida" diretamente nas câmaras/equipamentos externos, onde é carregado *firmware* específico, contendo cerca de 300.000 posições previsíveis do que poderá ser um elemento de alarme, normalmente pessoa ou veículo, e, com estes dados, permitindo o estabelecimento de regras sobre os mesmos para atuar de forma praticamente imediata sobre a imagem visualizada (com necessidade de um determinado movimento para se proceder à análise inteligente de vídeo – conjugação com posições previsíveis – normalmente entre 1 a 2 segundos de captação, no pressuposto de que uma imagem estática é passível de desclassificação pelo motor de analítica).
Quarta Fase (Atual)	
Sistemas com CNN (*convolutional neural networks*)	O mundo real é "ensinado" aos equipamentos, por forma a que percebam o que é "normal" numa determinada situação e o que é "anormal". Neste sistema não será necessário tempo para a conjugação de resultados possíveis, na medida em que os objetos estão classificados mesmo que estejam sem atividade. O tempo de resposta às regras pré-definidas (ou não, dado que o sistema identifica, também, anomalidades) é imediato e os falsos positivos quase inexistentes.

Fonte: Pessoa, entrevista, 08.04.2022.

Apêndice C – Matriz de análise das entrevistas – nível institucional

Tendo sido aplicadas entrevistas semiestruturadas, ao nível institucional, entre FS congéneres[1], apresenta-se a sua análise:

Quadro 11 – Matriz de análise das entrevistas semiestruturadas - FS congéneres

Conceitos/ Dimensões	**Perguntas/** Variáveis	**Códigos/** Segmentos de resposta	**E1**	**E2**	**E3**	**E4**	**E5**	**%**
Policiamento - Policiamento Preditivo (PP)	**1.** Realização de PP	**A.** Sim.			X	X		40
	2. Recolha de Informações Policiais	**A.1.2.** Sim. Utilização de Sistemas Informáticos.	X	X	X	X	X	**100**
	3/4. Análise de Dados	**A.2.1.** Sim. Relatórios de Informações.	X	X	X	X	X	**100**
		A.2.2. Sim. Mapas de Risco da Criminalidade.	X	X	X	X	X	**100**
		A.2.3. Sim. Utilização de Sistemas Informáticos de Informações Criminais interoperáveis - Partilha de Informações.	X	X	X	X	X	**100**
		A.2.3. Sim. Utilização de Sistemas Informáticos de Informações Criminais interoperáveis - Despacho de meios policiais.						0
	5/6/7. Policiamento orientado pela análise de Informações Policiais	**A.3.1.** Sim. Realização de ações de policiamento.	X	X	X	X	X	**100**
		A.3.2. Sim. Diminuição da taxa de crime.	X	X		X	X	80
		A.3.3. Sim. Rentabilização dos recursos policiais.	X		X		X	60
Videovigilância - Videovigilância Policial	**8.** Implementação de videovigilância policial	**B.** Sim.	X		X	X	X	80
	9/10. Tratamento e análise de dados	**B.1.1.** Características dos equipamentos. Lista de recursos e requisitos mínimos.			X		X	40
		B.1.2. Sim. Aplicação de IA.				X		20
	11/12/13. Maximização da atuação policial	**B.2.2.** Sim. Conexão a Bases de Dados de IC.				X		20
		B.2.1. Sim. Capacidade preditiva.	X	X	X	X	X	**100**
		B.2.1. Maximização da atuação policial.	X			X	X	60
		B.2.2. Rentabilização dos meios policiais.	X		X		X	60
Inteligência Artificial -	**14/15.** Recolha, tratamento e análise de dados	**C.1.1.** Sim. Aplicações de identificação de perfis de suspeitos.						0

[1] Entrevista aplicada às FS congéneres, com excertos de resposta, em Apêndice D.

Analítica de Vídeo		**C.1.2.** Sim. Aplicações de análise de movimentos e deteção de padrões suspeitos.						0
		C.1.3. Sim. Aplicações de controlo de tráfego.						0
		C.1.1/C.1.2/C.1.3. Sim. Mais valias.	X	X	X	X	X	**100**
Proteção de Dados - RGPD	**16/17/18.** Proteção dos DLG	**D.1.1.** Sim. Avaliação do impacto na privacidade. RGPD.	X	X	X	X	X	**100**
		D.1.2. Sim. Garantias e medidas para proteção de dados pessoais, conforme ordenamento jurídico.	X	X	X	X	X	**100**
		D.1.3. Sim. Entidade responsável pelos direitos de acesso e retificação dos dados pessoais.	X	X	X	X	X	**100**
	19/20. Cumprimento da regulamentação europeia	**D.2.1.** Sim. Medidas transpostas.	X			X	X	60
		D.2.2. Sim. Procedimentos internos para salvaguarda da aplicação de IA nos sistemas.		X	X		X	60

Fonte: Adaptado a partir de Moleirinho, 2021, p. Apd H-5.

Apêndice D – Guião A | Entrevista nível institucional - excertos de resposta

Quadro 12 – Excertos de respostas – Entrevistas nível institucional

Entrevistado	Pergunta e excerto da resposta	Segmento
Pergunta 1 - A Força adota o Policiamento Preditivo?		
E1	"Existem projetos, mas ainda não em prática."	**A.3.1**
E2	"Sim. Foi desenvolvida uma ferramenta baseada em IA para análise preditiva, para antecipar as ocorrências e evitar o efeito black box."	**A.3.1**
E3	"Sim. Num alcance limitado. Por exemplo, através da utilização de informação a partir de fontes abertas, para prever eventos e para otimizar o planeamento e emprego de forças operacionais (num horizonte temporal de um par de dias ou semanas)."	**A.3.1**
E4	"Não".	**A.3.1**
E5	"Não".	**A.3.1**
Pergunta 2 - No âmbito da recolha de informações policiais, a Força faz utilização de Sistemas Informáticos, metodologias, ferramentas e procedimentos específicos? Quais?		
E1	"Sim. O principal é o Sistema SIGO (Sistema Integrado de Gestión Operativa – Sistema Integrado para a Gestão Operacional), em que são registados todos os eventos, tarefas, relatórios de ocorrências e serviços, e inclui interface de pesquisa."	**A.1.1** **A.1.2**
E2	"Sim. Sistemas baseados na obtenção de dados – análise preditiva, autenticação deepfake e reconhecimento de discurso (em desenvolvimento)."	**A.1.1** **A.1.2**
E3	"Sim. A informação é obtida através dos operacionais e em colaboração com outras organizações no domínio da Segurança."	**A.1.1** **A.1.2**
E4	"Sim. Integração de dados de domínio transversal, recolha de relatórios de crime, análise de estatísticas de crime".	**A.1.1** **A.1.2**
E5	"Sim. O SIIOP (Sistema Integrado de Informações Operacionais Policiais), sistema baseado num repositório único, centralizado e alargado a todo o dispositivo, que permite à Guarda o suporte à decisão/ação, baseado em informação alargada e em tempo real, bem como a uniformização de procedimentos em toda a hierarquia.	**A.1.1** **A.1.2**
Pergunta 3 - No domínio da análise de dados, a Força produz relatórios de informações e elabora mapas de risco da criminalidade da sua área de responsabilidade?		
E1	"Sim. O SIGO pode elaborar mapas de risco da criminalidade, uma vez que todos os eventos são geolocalizados e têm uma marca de tempo."	**A.2.1** **A.2.2**
E2	"Sim. Através de sistemas automáticos de análise preditiva para elaborar mapas de risco da criminalidade."	**A.2.1** **A.2.2**
E3	"Sim. São produzidos relatórios sobre as tendências dos fenómenos criminais."	**A.2.1** **A.2.2**
E4	"Sim. No entanto, trata-se de uma função conjunta (partilhada)."	**A.2.1** **A.2.2**
E5	"Sim."	**A.2.1** **A.2.2**

Pergunta 4 - Faz utilização de Sistemas Informáticos de Informações Criminais interoperáveis com outras Entidades no setor da Segurança, ao nível nacional, para partilha de informações e direcionamento de meios policiais?		
E1	"Sim. Contudo o SIGO não se destina ao despacho de meios."	**A.2.3**
E2	"Sim. De forma muito limitada, por aspetos legais."	**A.2.3**
E3	"Sim. Apesar de, por vezes, com acesso limitado a outros sistemas."	**A.2.3**
E4	"Sim".	**A.2.3**
E5	"Sim". Para partilha de Informações. Plataforma PIIC.	**A.2.3**
Pergunta 5 - A Força realiza ações de policiamento orientado pela análise de informações policiais?		
E1	"Sim. As estatísticas são analisadas aos níveis local e central, para avaliar riscos e ameaças."	**A.3.1**

E2	"Sim. Apesar da importância de manter a decisão humana, a par da utilização dos sistemas automáticos."	**A.3.1**
E3	"Sim. Mas, atualmente, muito limitado."	**A.3.1**
E4	"Sim."	**A.3.1**
E5	"Sim."	**A.3.1**
Pergunta 6 - Nos locais de realização destas, verificou-se uma diminuição da taxa de criminalidade?		
E1	"Sim."	**A.3.2**
E2	"Sim. Mas é importante analisar o impacto das ações de prevenção e de repressão."	**A.3.2**
E3	"Não respondido."	**A.3.2**
E4	"Depende do tipo de crime".	**A.3.2**
E5	"Em muitos casos, sim."	**A.3.2**
Pergunta 7 - Estas ações de policiamento promovem a rentabilização dos recursos policiais?		
E1	"Sim."	**A.3.3**
E2	"Depende, da prioridade. O maior interesse recai sobre a promoção da eficiência e da transformação na forma de atuar, sendo mais fácil compreender o crime com métodos de análise preditiva e de justificar as ações (autoridades e cidadãos), alocando os meios certos em antecipação."	**A.3.3**
E3	"Sim. Permitem o emprego de recursos de forma mais eficiente e eficaz."	**A.3.3**
E4	"Não respondido".	**A.3.3**
E5	"Sim."	**A.3.3**
Pergunta 8 - A Força implementa sistemas de videovigilância policial em espaços públicos, na sua área de responsabilidade?		
E1	"Sim."	**B.1.1**
E2	"Não."	**B.1.1**
E3	"Sim. Por exemplo, em aeroportos."	**B.1.1**
E4	"Sim."	**B.1.1**
E5	"Sim. Em particular para a manutenção da segurança e ordem públicas, bem como a prevenção e dissuasão da prática de crimes."	**B.1.1**
Pergunta 9 - No domínio do tratamento e análise de dados, quais as especificações técnicas dos equipamentos de videovigilância, incluindo características que visem salvaguardar a recolha de imagem e de som em zonas privadas, que afetem a privacidade das pessoas e os seus Direitos, Liberdades e Garantias, conforme o ordenamento jurídico em vigor?		
E1	"A legislação nacional estabelece que a resolução que autoriza deve incluir os recursos das câmaras, contudo, não existe uma lista que exija recursos mínimos específicos."	**B.1.1**
E2	"A instalação de videovigilância está sujeita a controlo e a aspetos legais específicos."	**B.1.1**
E3	"Os dados são armazenados num sistema seguro e automaticamente eliminados após um número de dias definido."	**B.1.1**
E4	"Não respondido".	**B.1.1**
E5	"Em termos técnicos, os equipamentos de videovigilância devem apresentar as suas especificações de forma a identificar corretamente a forma de recolha, transmissão e conservação das imagens, a fim de garantir a confidencialidade, a autenticidade e integridade das imagens gravadas, com vista a garantir os Direitos, Liberdades e Garantias dos cidadãos, bem como a devida auditoria ao sistema pela CNPD. Nesse sentido, devem reunir, pelo menos, as características que permitam: • A Utilização exclusiva pela GNR • O acesso ao sistema de visualização mediante a atribuição de perfis de acesso RNSI. • As imagens encriptadas desde a câmara até ao militar que efetua a sua visualização; • Nas câmaras fixas, a existência de software para bloquear a filmagem de locais privados, com janelas ou entradas de edifícios, como principalmente o seu interior;	**B.1.1**

	• A impossibilidade de criação de perfis ou discriminação de pessoas, conforme previsto no artigo na Lei n.º 59/2019, de 8 de agosto de 2019; • A gravação dos dados registados apenas em meios físicos colocados exclusivamente à disposição da GNR; • Nos dados captados constar, de forma inequívoca, a data, a hora e o local da captura dos mesmos; • Conservar os dados em registo codificado, pelo prazo máximo de 30 dias contados desde a respetiva captação. Caso exista recurso a analítica de vídeo, devem existir um conjunto de regras para os utilizadores deste tipo de tecnologia, incluindo formação, no sentido de limitar a criação de perfis e o risco de discriminação e de violação do art.º 6 da Lei 59/2019, nomeadamente, pela capacidade desta tecnologia poder criar padrões de pesquiza pela análise de imagens. Importa que exista um conjunto de critérios e quem é o responsável pela definição de regras a aplicar.”	
Pergunta 10 - É aplicada Inteligência Artificial para tratamento e análise dos dados?		
E1	“Não.”	**B.1.2**
E2	“Depende, do caso e dos aspetos legais.”	**B.1.2**
E3	“Ainda não.”	**B.1.2**
E4	“Sim”.	**B.1.2**
E5	“Não. Contudo, desde que autorizado, os sistemas permitem a gestão analítica dos dados captados, mediante aplicação de critérios técnicos e de acordo com os fins a que os sistemas se destinam, sem nunca poderem, por imposição legal, captar e tratar dados biométricos.”	**B.1.2**
Pergunta 11 - Considera que a implementação de videovigilância policial em espaços públicos maximiza a atuação policial e pode contribuir para a capacidade preditiva?		
E1	“Sim.”	**B.2.2**
E2	“Depende, do que se pretende com tais sistemas. A tecnologia baseada em IA oferece muitas possibilidades, mas o uso legal é muito limitado.”	**B.2.2**
E3	“Sim.”	**B.2.2**
E4	“Sim”.	**B.2.2**
E5	“Sim, maximiza a capacidade de atuação policial, no entanto, a capacidade preditiva não é totalmente rentabilizada porque está dependente da utilização de software para analítica de vídeo ou mesmo de inteligência artificial, que se encontra impedido para o tratamento de dados biométricos. A capacidade preditiva destes sistemas terá de ter em conta as limitações legais e encontrar formas de utilizar os dados para o policiamento.”	**B.2.2**
Pergunta 12 - Os sistemas implementados pela Força estão ligados a Bases de Dados de Informações Criminais?		
E1	“Não.”	**B.2.1**
E2	“Não.”	**B.2.1**
E3	“Não.”	**B.2.1**
E4	“Sim”.	**B.2.1**
E5	“Não.”	**B.2.1**
Pergunta 13 - O que pode complementar relativamente ao potencial da implementação destes sistemas com ligação a estas Bases de Dados?		
E1	“Potenciaria as possibilidades de localizar pessoas desaparecidas, vítimas de crimes, assim como pessoas com medidas restritivas (alertas do SIS – verificações e mandados de prisão).”	**B.2.1** **B.2.2**
E2	“Nada a referir.”	**B.2.1** **B.2.2**
E3	“Nada a referir.”	**B.2.1** **B.2.2**
E4	“Renovado e implementado recentemente. O sistema é fortemente centrado nas necessidades de investigação”.	**B.2.1** **B.2.2**
E5	“Os dados dos sistemas de videovigilância podem contribuir para a produção de Informações, importantes para reunir conhecimento a	**B.2.1** **B.2.2**

	aplicar no planeamento do policiamento e prevenção criminal. No entanto, estes sistemas incidem primariamente na dissuasão e repressão de comportamentos criminais, colocados em locais onde existe necessidade de aplicar medidas preventivas e de apoio à decisão na gestão operacional de recursos."	
Pergunta 14 - Na aplicação de Inteligência artificial em sistemas de videovigilância policial em espaços públicos, pela Força, é feita utilização de aplicações de identificação de perfis de suspeitos, de análise de movimentos e deteção de padrões suspeitos e/ou de controlo de tráfego?		
E1	"Não."	**C.1.1** **C.1.2** **C.1.3**
E2	"Depende, do caso e dos aspetos legais."	**C.1.1** **C.1.2** **C.1.3**
E3	"Ainda não. Estão a ser desenvolvidas experiências e protótipos neste domínio, especialmente na análise de movimentos e deteção de padrões suspeitos."	**C.1.1** **C.1.2** **C.1.3**
E4	"Não".	**C.1.1** **C.1.2** **C.1.3**
E5	"De momento não. Mas poderão vir a ser utilizados na análise de movimentos e deteção de padrões suspeitos e/ou de controlo de tráfego, dentro dos limites da Lei."	**C.1.1** **C.1.2** **C.1.3**
Pergunta 15 - No seguimento da questão anterior, considera <u>tal utilização uma mais-valia</u>? Em que medida?		
E1	"Sim. A videovigilância e a conexão com bases de dados criminais (europeus ou nacionais) multiplicaria a eficácia das Agências de Aplicação da Lei."	**C.1.1** **C.1.2** **C.1.3**
E2	"Sim. Apenas em casos específicos (grandes eventos), em espaço e tempo limitados."	**C.1.1** **C.1.2** **C.1.3**
E3	"Sim. Detetar padrões suspeitos tem valor acrescentado na previsão e prevenção de criminalidade grave."	**C.1.1** **C.1.2** **C.1.3**
E4	"Baixa taxa de falsos positivos, Curva Característica de Funcionamento do Recetor aceitável e matriz de confusão em cenários de ambiente de elevada concentração de pessoas".	**C.1.1** **C.1.2** **C.1.3**
E5	"Sim. A gestão de vídeo com aqueles fins permite notificações em tempo real de eventos, comportamentos ou incidentes críticos que levam a um melhor emprego operacional e à prevenção comportamentos ilícitos. Face às dinâmicas atuais, são ainda fundamentais no apoio à decisão na atividade operacional das forças e serviços de segurança."	**C.1.1** **C.1.2** **C.1.3**
Pergunta 16 - No que respeita à proteção de dados pessoais e à salvaguarda dos Direitos, Liberdades e Garantias dos cidadãos, a Força, na implementação de sistemas de videovigilância policial em espaços públicos, desenvolve uma avaliação do impacto das operações de tratamento de dados dos cidadãos, incluindo, nomeadamente: **- Operações de tratamento de dados previstas;** **- Avaliação dos riscos para os Direitos, Liberdades e Garantias;** **- Medidas para mitigar os riscos identificados.**		
E1	"Sim. A legislação nacional estabelece essa necessidade."	**D.1.1**
E2	"Sim, conforme indicado."	**D.1.1**
E3	"Sim. Análise do impacto de privacidade, para salvaguardar a privacidade e os direitos humanos dos cidadãos. Estão a ser desenvolvidos métodos de anonimização para imagens de vídeo como meio de proteção da privacidade."	**D.1.1**
E4	"Sim. Em cumprimento do RGPD".	**D.1.1**
E5	"Sim. É um imperativo legal decorrente do art.º 29º da Lei 59/2019."	**D.1.1**

Pergunta 17 - No mesmo domínio da questão anterior, a Força assegura garantias, medidas de segurança e mecanismos para assegurar a proteção de dados pessoais e a conformidade do tratamento, de acordo com o ordenamento jurídico em vigor, incluindo: **- Controlo de custódia (capacidade de auditoria sobre os dados acedidos - quem, quando, onde e o quê);** **- Controlo de acesso ao equipamento;** **- Controlo dos suportes de dados;** **- Controlo da conservação dos dados;** **- Controlo dos utilizadores;** **- Controlo do acesso aos dados;** **- Controlo da comunicação;** **- Controlo da introdução;** **- Controlo do transporte;** **- Recuperação, fiabilidade e integridade.**		
E1	"Sim. Para qualquer atividade de processamento de dados."	**D.1.2**
E2	"Sim."	**D.1.2**
E3	"Sim. O acesso a dados pessoais é estritamente controlado, sendo apenas possível a quem tem o direito e a necessidade operacional de o fazer. Os dados só podem ser armazenados para investigação caso exista um fundamento legal."	**D.1.2**
E4	"Sim."	**D.1.2**
E5	"Sim. Todas estas medidas devem ser asseguradas conforme previsto nas Lei 59/2019, de 08 de agosto e Lei 95/2021, de 29 de dezembro."	**D.1.2**
Pergunta 18 - Na mesma linha do referido anteriormente, está definida uma Entidade responsável pelo cumprimento, exercício dos direitos de acesso e retificação dos dados, ao nível da Força?		
E1	"Sim. Os cidadãos são informados sobre a quem dirigir os pedidos de direitos de acesso e eliminação."	**D.1.3**
E2	"Sim. Uma equipa DPO e um administrador de dados, códigos e algoritmos."	**D.1.3**
E3	"Sim."	**D.1.3**
E4	"Sim."	**D.1.3**
E5	"Sim. Por norma é o responsável pela utilização do sistema."	**D.1.3**
Pergunta 19 - Quais as medidas decorrentes da transposição nacional da regulamentação europeia, neste domínio?		
E1	"Sim. As decorrentes da transposição nacional da Diretiva europeia (Diretiva 680/2016)."	**D.2.1**
E2	"Em discussão."	**D.2.1**
E3	"Não respondido."	**D.2.1**
E4	"Comunicação à Autoridade, gestão de dados, responsável pela proteção de dados."	**D.2.1**
E5	"Apenas a aplicação do ordenamento jurídico relativamente à videovigilância em espaços públicos e à proteção de dados."	**D.2.1**
Pergunta 20 - Quais os procedimentos desenvolvidos internamente, pela Força, para salvaguarda do cumprimento da regulamentação europeia, na aplicação de Inteligência Artificial em sistemas de videovigilância policial em espaços públicos?		
E1	"Existe uma proposta de regulamentação da UE para aplicação de IA. No entanto, ainda não existe nenhum sistema implementado."	**D.2.2**
E2	"Os procedimentos legalmente previstos."	**D.2.2**
E3	"Relativamente à IA, foi desenvolvido o Manifesto Ético, onde são especificadas as diretrizes éticas seguidas e como são acompanhadas as possíveis questões neste âmbito, o qual é baseado nos regulamentos europeus e inclui uma versão do jogo Judgement Call, da Microsoft. Adicionalmente, o trabalho é desenvolvido em estreita colaboração com advogados experientes na área da análise de dados para fins policiais."	**D.2.2**
E4	"Não respondido".	**D.2.2**
E5	"De momento, a legislação nacional já contempla as orientações necessárias na Lei 95/2021, de 29 de dezembro, pelo que, os procedimentos serão de acordo com a mesma."	**D.2.2**

Apêndice E – Guião B | Entrevista nível político - excertos de resposta

Dr. Antero Luís (resposta formal do Gabinete)
Secretário de Estado Adjunto e da Administração Interna

Pergunta n.º 1. Considera importante a aplicação de IA para o tratamento e análise de dados recolhidos no âmbito da videovigilância policial? Em que medida?

Resposta	"A utilização de IA no âmbito do trabalho policial é uma matéria que tem gerado debate no espaço público, com alguma controvérsia e também alguma desinformação, pelo que deve ser abordada com a maior seriedade, mas também com grande prudência. Com seriedade, pois estamos a falar da aplicação de tecnologia que pode contribuir decisivamente para a melhoria da eficácia e eficiência do trabalho policial e potenciar a melhoria da segurança pública. Com prudência, porque falamos de uma ferramenta que, usada incorretamente, pode impactar diretamente na esfera da vida pessoal dos cidadãos e afetar os direitos liberdade e garantias, que, em última análise, todos queremos proteger. Por isso, a utilização da IA não poder deixar de ser previamente balizada pela lei, prevendo, com precisão, a sua admissibilidade e as condições e as formas da sua utilização, bem como os limites a essa mesma utilização. Ao mesmo tempo devem ser previstos os necessários mecanismos de controlo que previnam e impeçam que desta utilização possa resultar, de forma desproporcional, impacto ou dano para os direitos fundamentais dos cidadãos."

Pergunta n.º 2. De que forma a aplicação de IA poderá contribuir para salvaguardar os DLG dos cidadãos e a proteção dos dados tratados?

Resposta	"Quando falamos da aplicação de inteligência artificial no âmbito da segurança interna estamos a falar, genericamente, da utilização de meios tecnológicos ao serviço do sistema de segurança interna, nomeadamente das forças e serviços de segurança, como um meio auxiliar ou adicional ao desempenho da sua missão, legal e constitucionalmente consagrada. Como resulta da CRP (artigo 272.º) a função da polícia (polícia aqui entendida no seu sentido mais lato, englobando todos os órgãos que desenvolvem atribuições de polícia, nomeadamente as forças e serviços de segurança) compreende a defesa da legalidade democrática a garantia da segurança interna e dos direitos dos cidadãos. Nos termos da LSI, a segurança interna mais não é do que a atividade desenvolvida pelo Estado para garantir a ordem, segurança e tranquilidade publicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o no e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias dos cidadãos e o respeito pela legalidade democrática (Cfr. artigo 1.º da Lei n.º 53/2008, de 29 de agosto). Importa lembrar também que o direito à segurança previsto no artigo 27.º da CRP, se insere no capítulo do direitos, liberdades e garantias pessoais. Desta forma a aplicação de IA no âmbito da segurança interna, por exemplo a sua na utilização nos sistemas de videovigilância, só pode ser entendida como um contributo para a salvaguarda dos direitos dos cidadãos, nomeadamente na salvaguarda do direito à segurança, cuja garantia é uma tarefa fundamental do Estado (Cfr. artigo 9.º da CRP). Como já foi referido, a utilização da IA no âmbito da segurança interna, tal como em qualquer outra atividade do Estado, não pode deixar de respeitar os princípios constitucionais que enformam essa atividade, nomeadamente o princípio da proporcionalidade, evitando que essa utilização seja ela própria violadora dos direitos que se pretendem salvaguardar."

Pergunta n.º 3. Quais os critérios e pressupostos técnicos que devem ser aplicáveis aos sistemas de IA, de acordo com os fins a que destina?

Resposta	"Quando estamos a falar dos sistemas de videovigilância utilizados pelas forças e serviços de segurança, enquadráveis na Lei n.º 95/2021, de 29 de dezembro, existe efetivamente a possibilidade de o tratamento de dados ter subjacente um sistema de gestão analítica de dados, por aplicação de critérios técnicos, de acordo com os fins a que se destinam os sistemas de videovigilância (Cfr. artigo 16.º da lei atrás referida). A descrição dos critérios técnicos utilizados no sistema de gestão analítica dos dados captados, é obrigatoriamente incluída na documentação que compõe a instrução de cada um dos pedidos de autorização

	de sistemas de videovigilância, que pretendam utilizar tais sistemas de gestão analítica de dados, como decorre da alínea b) do n. º1 do artigo 6.º da Lei n.º 95/2021. Os critérios técnicos são assim objeto de definição, prévia à autorização de instalação dos sistemas, e são matéria objeto do parecer obrigatório da Comissão Nacional de Proteção de Dados (CNPD), como resulta do n.º 3 do artigo 5.º do mesmo diploma legal. Dito isto, os critérios e pressupostos técnicos, a definir previamente e adaptados a cada um dos fins a que os sistemas se destinam, terão obrigatoriamente que respeitar os comandos constitucionais e legais que enformam a proteção de dados. Ainda sobre este assunto será importante referir que ainda não foi publicada a regulamentação da lei em apreço, sendo expectável que essa regulamentação venha trazer orientações sobre os requisitos técnicos que a solução analítica de dados deve observar.”

Pergunta n.º 4. **Em que situações poderia ser admissível a utilização de sistemas para identificação biométrica em tempo real?**

Resposta	“No que diz respeito aos sistemas de videovigilância enquadráveis na Lei n.º 95/2021, de 29 de dezembro, o n.º 2 do artigo 16.º é claro ao proibir que os sistemas de gestão analítica de dados, permitam captar ou tratar dados biométricos.”

Pergunta n.º 5. **Quais os mecanismos e procedimentos que possam mitigar os riscos associados aos sistemas de IA, sobretudo os que reúnem capacidade de tratar dados biométricos, assim como os requisitos necessários, designadamente à qualidade dos dados, à documentação técnica, aos registos, à transparência, à supervisão humana, à solidez, à exatidão e à cibersegurança?**

Resposta	“No âmbito dos sistemas de videovigilância, aqui considerados, a própria lei prevê a existência de mecanismos destinados à mitigação de riscos associados à utilização de tais sistemas. Desde logo a obrigatoriedade de inclusão da descrição dos critérios utilizados no sistema de gestão analítica de dados, na instrução do processo a submeter à entidade que autoriza (Cfr. artigo 6.º n.º 1 alínea g), garantindo assim uma validação prévia. Tais critérios são também objeto de análise da CNPD (n.º 3 do artigo 5.º, com uma referência direta ao artigo 16.º), o que reforça a verificação prévia à autorização e à sua validação. Para além do referido, importará ainda ter presente que para este efeito, mitigar riscos, a Lei n.º 95/2021 prevê ainda outros mecanismos como por exemplo: o n.º 3 do artigo 4.º, ou os artigos 20.º, 21.º, 24.º e 26.º.”

Apêndice F – Guião C | Entrevista nível técnico - excertos de resposta

Gonçalo Pereira Pessoa
Motorola Solutions | Avigilon - Video Security & Access Control

Pergunta n.º 1. **Considera importante a aplicação de IA para o tratamento e análise de dados recolhidos no âmbito da videovigilância policial? Em que medida?**

Resposta	"Sim, na medida em que a conjugação da recolha de imagens e da capacidade de as analisar e criar um tipo de ação ou alerta, com base no resultado, exponencia as operações de segurança, no que se refere à eficácia e à eficiência dos recursos. Sendo sempre fundamental e indissociável a intervenção humana para a validação final do resultado obtido e prossecução dos passos seguintes, não permitindo nunca que a operação de IA suplante o fator humano de decisão e sua respetiva supervisão e auditoria."

Pergunta n.º 2. **De que forma a aplicação de IA poderá contribuir para salvaguardar os DLG dos cidadãos e a proteção dos dados tratados?**

Resposta	"Cumprindo a Constituição em toda a sua plenitude, bem como às leis que dela emanam, sendo supervisionada e auditada a todo o momento, além de garantir que nenhum meio automático e/ou autónomo por si só, gerador de eventos ou alarmes, tome decisões que possam contornar ou assumir uma responsabilidade exclusiva de um ser humano, e que por fim, não intervenha nas decisões que cabem ao operador / supervisor, mas sim que as auxilie no decurso da operação e apresente resultados rápidos e fiáveis para as tomadas das respetivas decisões. Os elementos, operador e supervisor, - numa perspetiva positiva a adicionar à um futuro diploma regulador (Portaria)-, deveriam ser certificados nas operações de vigilância com IA ou atividades relacionadas com IA que interferem na esfera pública. Estes elementos, quando relacionados com proteção pública (videovigilância, intervenções, gestão de conflitos), serão passíveis de auditoria, tendo o seu âmbito de atuação regulada com os estatutos próprios, e que até já são comuns ao juramento prestado à bandeira e ao país, não havendo dissonância de maior. Assim sendo, como de uma atuação física se tratasse, a operação com elementos de IA, teria o mesmo grau de responsabilização que uma atuação presencial de um agente no cumprimento dos DLG dos cidadãos. Carece, pois, que o legislador se detenha nos pormenores de um eventual diploma e que façam disto uma realidade para uma melhor e eficaz atuação das forças de segurança, não só pela carência cada vez maior de elementos para os quadros como também pela fiabilidade atual das soluções de IA, que permitem uma conjugação única entre custo / benefício."

Pergunta n.º 3. **Quais os mecanismos e procedimentos que possam mitigar os riscos associados aos sistemas de IA, assim como os requisitos necessários, designadamente à qualidade dos dados, à documentação técnica, aos registos, à transparência, à supervisão humana, à solidez, à exatidão e à cibersegurança?**

Resposta	"Existe um encadeamento orgânico legislativo que regula as atividades das forças de segurança bem como o advento de determinadas fraudes que têm por base crimes no ciber espaço. Assim, grande parte da legislação existente é adaptável, com elementos obviamente mais atuais, a uma legislação mais próxima da realidade da IA, na estrita observância dos DLG. O grande desafio seria transpor estas legislações, que relevam um caráter físico imediato de intervenção, para uma intervenção contínua e remota, sendo acionados os meios quando se justifiquem bem como a investigações à posteriori, rápida e simplificada. Como pontos de boas práticas que poderiam ser plasmados num eventual diploma poder-se-ia enumerar: 1) Gestão por operadores e supervisores certificados 2) Investigação e/ou extração de imagens sempre com dupla autenticação (senha e QR code por exemplo) (operador +supervisor) de forma presencial. 3) Auditoria do sistema de 6 em 6 meses por entidade de segurança treinada para o efeito, com foco principal: a) Na gestão do sistema instalado e se cumpre integralmente com as leis em vigor

	b) Nas infraestruturas físicas (cablagens) e de ligação de ativos de redes e sua forma de conexão, com o intuito de certificar que o canal de comunicação entre a captação, gravação e gestão (operação do sistema), se mantém inviolável. c) Nas infraestruturas lógicas (sistemas) e de ligação de ativos de redes e sua forma de conexão, com o intuito de certificar que o canal de comunicação entre a captação, gravação e gestão (operação do sistema), se mantém inviolável e encriptada. d) Que não haja qualquer tipo de alteração ao previsto pela CNPD, seja pela autorização de utilização ou por um eventual parecer. 4) A qualquer momento ser passível de uma intervenção remota por quadros credenciados de topo, por questões de segurança interna, devidamente fundamentado (ataques terroristas, ou preparação de ataques terroristas, procura de suspeitos internacionais (credenciados na Interpol ou Europol) e que exijam colaboração com Estados vinculados, entre outros). 5) O sistema ser passível de ter todos os registos auditáveis dentro do limite legal de 30 dias, sendo a auditoria feita pelas entidades credenciadas de forma aleatória ou programada. Os dados deverão estar sempre consistentes e invioláveis. 6) Garantir que o sistema seja integral de um fabricante para facilitar a gestão e auditoria bem como as definições de segurança dos sistemas evitando múltiplos sistemas numa mesma instalação que torne impossível dirimir responsabilidades. 7) Base de dados própria e encriptada (não deverá ser do tipo SQL dado as vulnerabilidades que existem com as mesmas, em grande parte devido à sua popularidade), mas uma que seja proprietária do fabricante e que esta base de dados não tenha custos e pertença ao cliente (força de segurança) para não criar dependências de terceiros na gestão da mesma. Da mesma forma que um sistema operativo do fabricante e que seja baseado em Linux ajudará a inviolabilidade dos dados pois não serão visíveis para futuros ataques cibernéticos, como ocorrem com a maior parte dos sistemas instalados.”

Pergunta n.º 4. Quais os critérios utilizados atualmente no sistema de gestão analítica dos dados captados no âmbito da videovigilância policial?

Resposta	“Os critérios atuais são regidos pelas leis em vigor que não contemplam o tratamento de metadados como tal, ou seja, que permitam identificar de maneira inequívoca uma pessoa e correlacioná-la durante um determinado período de tempo. Poder-se-á argumentar que os sistemas que utilizamos (disclaimer: Motorola Solutions) não estão vinculados aos metadados pois pela definição o metadado, esta é a descrição ou conjunto de características de um dado ou item, e no nosso casso todos os dados são arquivados como uma encriptação fotograma à fotograma que compõem uma determinada imagem sem descrição, sem vínculo bidirecional. O vínculo só é dado quando o operador e/ou supervisor aciona as “pesquisas por aparência” sendo que o seu resultado é a apresentação de diversas imagens semelhantes, mas não vinculativas. Cabe ao operador e/ou supervisor fazer a respetiva identificação afirmativa ou não e continuar a sua investigação, tal e qual de uma no terreno se tratasse. Ou seja, a gestão dos dados não são vinculativas, nem tão pouco violáveis.”

Pergunta n.º 5. O que pode acrescentar sobre a evolução da Analítica de Vídeo e as possibilidades da sua aplicação com IA?

Resposta	“A evolução será tão positiva quanto for os requisitos de acesso as aplicações. Nesses requisitos estão, como mencionados acima: 1)O cumprimento de toda a legislação em vigor e/ou futuras, tendo por base a nossa constituição. 2)A formação de todos os elementos das forças de segurança que deverão operar o sistema. 3)A capacidade de auditoria dos elementos adstritos a esta função 4)A revisão e supervisão das leis e a sua adaptação a realidade atual e futura. 5)O poder de decisão final deverá ser sempre humano (operador e supervisor). Cumprindo estes requisitos basilares, os sistemas poderão garantir os nosso DLGs e estarem verdadeiramente ao serviço da sociedade e ao bem comum.”

Apêndice G – Proposta de boas práticas a implementar na GNR

Quadro 13 – Boas práticas propostas para o domínio da Fundamentação no pedido para implementação de sistemas de videovigilância policial em espaços públicos com IA

	Boas práticas	Finalidades/Especificação
DA FUNDAMENTAÇÃO	**Demonstração da necessidade e proporcionalidade da aplicação de IA**	– Demonstração da *imprescindibilidade*, à luz dos fins a que se destina o sistema, e da *proporcionalidade*, através da identificação concreta dos problemas, por exemplo, índices de criminalidade na área de incidência, e o impacto da utilização do sistema com IA nos resultados, com relação entre benefícios e prejuízos, em cumprimento da legislação); – *Transparência* na utilização dos dados, cumprindo a legislação (o sistema de IA não poderá tratar dados que não sejam autorizados); – Utilização da IA para garantia da proteção dos DLG dos cidadãos, em especial a proteção de dados pessoais, em sistema auditado, em cumprimento da legislação.
	Especificação dos critérios, circunstâncias e limites para a utilização de IA	– Estabelecimento das *condições objetivas de utilização*, designadamente, áreas de incidência da captação dos dados e a duração, e os fatores/situações que justificam o recurso ao algoritmo de análise de imagens, incluindo os que devem estar na base da seleção de pessoas e/ou veículos para rastreamento, como por exemplo, no âmbito da investigação criminal, a pesquisa de determinados elementos com características definidas, num local e tempo específico (definição do *conceito de utilização*, de acordo com os parâmetros legais); – Autoria prévia ao sistema, pela CNPD, para assegurar transparência e fiabilidade.
	Avaliação de impacto e demonstração da segurança e fiabilidade do sistema com aplicação de IA	– Levantamento do *impacto e riscos* sobre os DLG e definição de medidas mitigadoras, para salvaguarda da proteção de dados pessoais, demonstrando, nomeadamente, dados que permitam concluir que os resultados apresentados pelo sistema, sobre os quais as FS e o sistema judicial decidirão sobre cidadãos visados, não são discriminatórios e contrários aos princípios constitucionais; – Demonstração da estrutura de cibersegurança; – Manutenção do foco na demonstração da transparência e proporcionalidade do recurso à utilização de IA.
	Demonstração da permanente auditabilidade do sistema	Garantia da *segurança e fiabilidade*, e em especial os registos das operações de tratamento dos dados pessoais, por entidades certificadas.
	Inclusão dos termos do contrato com a Empresa responsável pela instalação, manutenção e substituição dos equipamentos	– Especificação das *funcionalidades* do sistema para a analítica de vídeo, com demonstração do cumprimento dos normativos legais, como forma de reforçar a transparência e a fiabilidade do sistema; – Garantia da *utilização exclusiva* do sistema pela FS, em matéria do seu domínio e controlo, para salvaguarda da segurança e da fiabilidade.

Quadro 14 – Boas práticas propostas para o domínio dos Requisitos Técnicos, no pedido para implementação de sistemas de videovigilância policial em espaços públicos com IA

	Boas práticas	Finalidades/Especificação
DOS REQUISITOS TÉCNICOS	**Identificação da forma de recolha, transmissão e conservação das imagens**	Em especial as *características* que permitam: – *Utilização exclusiva* do sistema pela FS (integral de um fabricante, para facilitar as definições de segurança e a responsabilização); – Acesso ao sistema de visualização e/ou extração de imagens mediante *perfis de acesso* e somente com sistema de *dupla autenticação* (senha e QR *code*, a título de exemplo), de forma *presencial*; – Aplicação de *software de filtros de ocultação* em locais privados e respetivos acessos (portas e janelas), que impeça a captação de imagem e de som – neste caso, devem ser assinaladas as zonas a filtrar nas áreas de incidência, assim como identificadas as câmaras e respetivos ângulos de visão; – *Encriptação das imagens*, desde a captação (na câmara) até à visualização destas, ou seja, em todo o canal de comunicação captação-gravação-gestão; – Arquivamento dos dados com *encriptação fotograma a fotograma*, compondo *imagens sem descrição e sem vínculo bidirecional*, apenas passível de ser atribuído mediante ação do agente operador e/ou supervisor do sistema, facilitando a gestão dos dados não vinculativa e promovendo a sua inviolabilidade; – *Gravação* dos dados registados somente *nos meios físicos* especificamente *definidos e autorizados*; – Inscrição, nos dados captados, de forma inequívoca, da data, hora, local e equipamento de captura; – Aplicação de *mecanismos de anonimização* para as imagens de vídeo, para impossibilidade de criação de perfis ou discriminação de pessoas; – *Conservação dos dados* captados em registo codificado, pelo prazo máximo de 30 dias, contados a partir da data de captação; – Mecanismos de segurança e proteção da rede e sistemas utilizados, como dos dados captados, a fim de não serem comprometidos por qualquer ciberameaça (estrutura de cibersegurança).
	Utilização de base de dados própria e encriptada	Garantia da segurança e fiabilidade do sistema.
	Uso de sistema operativo baseado em Linux	Facilitação da inviolabilidade dos dados (segurança).

Quadro 15 – Boas práticas propostas para o domínio das Medidas e Procedimentos, no pedido para implementação de sistemas de videovigilância policial em espaços públicos com IA

	Boas práticas	Finalidades/Especificação
DAS MEDIDAS E PROCEDIMENTOS PARA PROTEÇÃO DOS DADOS	**Definição de regras e critérios para utilização do sistema com aplicação de IA**	– Definição do conjunto de procedimentos para os operadores do sistema; – Definição de um responsável, contemplando, nomeadamente, a preservação de imagens extraídas, no âmbito da investigação criminal, incluindo como são excecionadas da rotatividade de 30 dias do arquivo do sistema, bem como a sua eliminação, após a conclusão do processo-crime.
	Segregação física e lógica das redes de videovigilância das outras redes	Aplicação de protocolo HTTPS, para garantia da segurança do sistema.
	Segurança física do sistema	– Inclusão de sistema *anti-tampering* nos armários de comunicações, com alertas, além da existência de plataformas de *software* que permitam acompanhar o estado dos equipamentos que interagem, como as câmaras, designadamente o *Site Health*; – Localização dos armários de comunicações em pontos que dificultem o acesso, nos locais públicos.
	Auditorias ao sistema	– Realização com caráter regular e programado, mas, também, inopinadamente; – Ao funcionamento do sistema, à estrutura de cibersegurança, ao registo das operações de tratamento dos dados e ao cumprimento dos procedimentos estabelecidos, relativamente à captação, acesso e tratamento - essencial registos cronológicos com detalhe do operador e o que fez; – Ao registo de todas as ações efetuadas por um utilizador, incluindo tentativas de acesso, assim como a obrigação de garantia da sua integridade, através de assinatura e *TimeStamp*.
	Contratação da instalação, manutenção e substituição dos equipamentos	A uma única Empresa, com absoluta garantia que a FS mantém em permanência o domínio e controlo da gestão do sistema e do tratamento dos dados.
	Sistema de cópias de segurança dos dados	– Garantia da disponibilidade dos dados, no prazo dos 30 dias, em caso de eliminação acidental, para além das condições previstas para a sua recuperação, em caso de avarias no armazenamento; – Quantificação de dois servidores, em cenário de *failover*, com a arquitetura de partilha da unidade dedicada a armazenamento de dados, assegurando, assim, a continuidade do sistema, em caso de falha no servidor ativo.
	Formação	Formação e credenciação específica aos operadores e gestores do sistema.
	Sistema de controlo de acessos às salas de tratamento de dados	Registo de entradas e saídas, no sentido de se poder demonstrar a imputabilidade de qualquer evento.