



Universidades Lusíada

Rola, Eulálio do Carmo da Silva, 1965-

Os principais contributos da inteligência artificial para o processamento de imagens digitais a utilizar na segurança pública

<http://hdl.handle.net/11067/6548>

Metadados

| | |
|---------------------------|---|
| Data de Publicação | 2022 |
| Resumo | <p>Este estudo apresenta uma visão de necessidade evolucionista, da atuação das Forças e Serviços de Segurança, na comparticipação produzida por alguns dos novos avanços da Inteligência Artificial, que vem mudar de forma radical, a conceção clássica de acesso e salvaguarda de dados em formato digital, tendo em vista contribuir de forma direta para o aumento da assertividade na Investigação Criminal, com reflexo direto na melhoria da manutenção da Segurança Pública. A Inteligência Artificial, permi...</p> <p>This study presents a vision of evolutionary need, the performance of the Security Forces and Services, in the participation produced by some of the new advances of Artificial Intelligence, which changes radically, the classic conception of access and safeguarding of data in digital format, with a view to contributing directly to the increase of assertiveness in Criminal Investigation, with a direct impact on improving the maintenance of Public Safety. The Artificial Intelligence, allows auto...</p> |
| Palavras Chave | Polícia - Inovações tecnológicas, Investigação criminal - Inovações tecnológicas, Inteligência artificial, Protecção de dados - Direito e legislação |
| Tipo | masterThesis |
| Revisão de Pares | Não |
| Coleções | [ULL-FD] Dissertações |

Esta página foi gerada automaticamente em 2024-07-18T10:20:22Z com informação proveniente do Repositório



UNIVERSIDADE LUSÍADA

FACULDADE DE DIREITO

Mestrado em Segurança e Justiça

**Os principais contributos da inteligência artificial para o
processamento de imagens digitais
a utilizar na segurança pública**

Realizado por:
Eulálio do Carmo da Silva Rola

Orientado por:
Prof. Doutor Luís Carlos Rodrigues Malheiro

Constituição do Júri:

Presidente: Prof. Doutor José Francisco Lynce Zagalo Pavia
Orientador: Prof. Doutor Luís Carlos Rodrigues Malheiro
Arguente: Prof. Doutor José Alberto Rodríguez Lorenzo González

Dissertação aprovada em: 17 de outubro de 2022

Lisboa

2022



U N I V E R S I D A D E L U S Í A D A

FACULDADE DE DIREITO

Mestrado em Segurança e Justiça

Os principais contributos da inteligência artificial para
o processamento de imagens digitais a utilizar na
segurança pública

Eulálio do Carmo da Silva Rola

Lisboa

Maio 2022



U N I V E R S I D A D E L U S Í A D A

FACULDADE DE DIREITO

Mestrado em Segurança e Justiça

Os principais contributos da inteligência artificial para
o processamento de imagens digitais a utilizar na
segurança pública

Eulálio do Carmo da Silva Rola

Lisboa

Maio 2022

Eulálio do Carmo da Silva Rola

Os principais contributos da inteligência artificial para
o processamento de imagens digitais a utilizar na
segurança pública

Dissertação apresentada à Faculdade de Direito da
Universidade Lusíada para a obtenção do grau de
Mestre em Segurança e Justiça.

Orientador:
Prof. Doutor Luis Carlos Rodrigues Malheiro

Lisboa

Maio 2022

FICHA TÉCNICA

Autor Eulálio do Carmo da Silva Rola
Orientador Prof. Doutor Luis Carlos Rodrigues Malheiro
Título Os principais contributos da inteligência artificial para o processamento de imagens digitais a utilizar na segurança pública
Local Lisboa
Ano 2022

MEDIATECA DA UNIVERSIDADE LUSÍADA - CATALOGAÇÃO NA PUBLICAÇÃO

ROLA, Eulálio do Carmo da Silva, 1965-

Os principais contributos da inteligência artificial para o processamento de imagens digitais a utilizar na segurança pública / Eulálio do Carmo da Silva Rola ; orientado por Luis Carlos Rodrigues Malheiro. - Lisboa : [s.n.], 2022. - Dissertação de mestrado em Segurança e Justiça, Faculdade de Direito da Universidade Lusíada.

I - MALHEIRO, Luís Carlos Rodrigues, 1986-

LCSH

1. Polícia - Inovações tecnológicas
2. Investigação criminal - Inovações tecnológicas
3. Inteligência artificial
4. Proteção de dados - Direito e legislação
5. Universidade Lusíada. Faculdade de Direito - Teses
6. Teses - Portugal - Lisboa

1. Police - Technological innovations
2. Criminal investigation - Technological innovations
3. Artificial intelligence
4. Data protection - Law and legislation
5. Universidade Lusíada. Faculdade de Direito - Dissertations
6. Dissertations, Academic - Portugal - Lisbon

1. HV8073.R65 2022

Uma imagem é mais do que mil palavras, um evento é mais do que milhares de fotografias. Um evento é a unidade básica de conhecimento que faz a ponte entre o mundo físico e os objetos semânticos.

YAN, Wei Qi (2019) - Introduction to intelligent surveillance : surveillance data capture, transmission, and analytics. 3th ed. Cham : Springer.

AGRADECIMENTOS

Ao Professor Dr. Luis Malheiro. pelos incontáveis conselhos e orientações, pela paciência, dedicação e confiança no meu trabalho. O seu grau de exigência e à sua forma peculiar de motivar inspira-me a ser um pesquisador cada vez melhor. À Eng.^a Nazare Teixeira, minha estimada leitora, pelas preciosas sugestões e atenciosos comentários. Aos colegas de curso Pedro Jardim, Carlos Dias, pelas frutíferas discussões, contribuições e incentivo.

Um especial agradecimento aos digníssimos entrevistados, por terem anuído e de igual pelo extraordinário contributo a ciência, com o vosso pensamento crítico.

Deixo igualmente os meus calorosos agradecimentos aos demais professores do curso de Mestrado em Segurança e Justiça da Universidade Lusíada de Lisboa.

A minha companheira Rita Vaccaro, pela prestimosa paciência e motivação positiva, na minha jornada neste mestrado. Aos meus filhos, Fábio, Daniel, Ruben, Joel, Miriam, que sempre me apoiaram e que lhes sirva de referência que, quem nos limita somos nós mesmos.

A Catarina Graça da Universidade Lusíada, por toda a dedicação, na imensa ajuda de revisão desta dissertação. Agradeço a todos que direta ou indiretamente contribuíram para mais esta conquista.

O analfabeto do século XXI não será aquele que não consegue ler e escrever, mas aquele que não consegue aprender, desaprender e reaprender.

TOFFLER, Alvin (1971) - Future shock. 3rd printing. New York : Bantam Book.

APRESENTAÇÃO

Os principais contributos da Inteligência Artificial para o processamento de imagens a utilizar na segurança pública

Eulálio do Carmo da Silva Rola

Este estudo apresenta uma visão de necessidade evolucionista, da atuação das Forças e Serviços de Segurança, na comparticipação produzida por alguns dos novos avanços da Inteligência Artificial, que vem mudar de forma radical, a conceção clássica de acesso e salvaguarda de dados em formato digital, tendo em vista contribuir de forma direta para o aumento da assertividade na Investigação Criminal, com reflexo direto na melhoria da manutenção da Segurança Pública.

A Inteligência Artificial, permite de forma autónoma, rastrear, identificar e informar com precisão, sobre pessoas, viaturas e diversos objetos num dado tempo e espaço, atuando como um aliado para potenciar a Segurança Pública, pela sua aplicação no processamento da análise digital dos registos de imagens, produzindo impacto na prevenção, auditoria criminal, concomitantemente no desempenho dos profissionais de segurança.

Assim, afigura-se como relevante estudar o uso destes instrumentos, para permitir que os órgãos políticos, a sociedade civil e as Forças e Serviços de Segurança, melhorem, encontrem, meios tecnológicos, para cumprir com crescente facilidade e agilidade, todos os pressupostos de eficácia e eficiência na securitização pública, mas, também observar a preservação dos direitos, liberdades e garantias dos cidadãos.

Palavras-chave: Inteligência Artificial, segurança pública, investigação criminal, imagem digital, telemóvel, profissional de segurança, dados, informações.

PRESENTATION

The main contributions of Artificial Intelligence to the processing of images to be used in public safety

Eulálio do Carmo da Silva Rola

This study presents a vision of evolutionary need, the performance of the Security Forces and Services, in the participation produced by some of the new advances of Artificial Intelligence, which changes radically, the classic conception of access and safeguarding of data in digital format, with a view to contributing directly to the increase of assertiveness in Criminal Investigation, with a direct impact on improving the maintenance of Public Safety.

The Artificial Intelligence, allows autonomously, to accurately track, identify and inform, about people, vehicles and various objects in a given time and space, acting as an ally to enhance Public Security, for its application in the processing of digital analysis of image records, producing impact on prevention, criminal audit, concomitantly in the performance of security professionals.

Thus, it seems relevant to study the use of these instruments, to allow political bodies, civil society and security forces and services to improve, find technological means, to comply with increasing ease and agility, all the assumptions of effectiveness and efficiency in public securitization, but also to observe the preservation of citizens' rights, freedoms and guarantees.

Keywords: Artificial intelligence, public security, criminal investigation, digital images, mobile phone, security professional, data, information.

LISTA DE TABELAS

| | |
|--|----|
| Tabela 1 - Entrevistados | 27 |
| Tabela 2 - Resumo Compton | 50 |
| Tabela 3 - Resumo <i>BriefCam</i> | 52 |

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

- 3D - Imagens tridimensionais
- 5G - Quinta geração de tecnologia de comunicações móveis
- AC - Auditoria Criminal
- CCC - Centro de Comando e Controle
- CCTV - Closed Circuit Television
- CNPD - Comissão Nacional de Proteção de Dados
- FSS - Forças e Serviços de Segurança
- GPS - Global position System (Sistema de Posicionamento Global)
- IA - Inteligência Artificial
- IC - Investigação Criminal
- IoT - Internet of Things (internet das coisas)
- JIC - Juiz de Instrução Criminal
- OS - Profissional de Segurança
- PS - Profissional de Segurança
- RAR - Reconhecimento Automático de Matrículas
- RGPD - Regulamento Geral de Proteção de Dados
- SP - Segurança Pública
- TI - Tecnologias de Informação

SUMÁRIO

| | |
|---|----|
| 1. Introdução | 21 |
| 1.1. Enquadramento..... | 21 |
| 1.2. Objetivos | 23 |
| 2. Metodologia de investigação | 25 |
| 2.1. Metodologia..... | 25 |
| 2.2. Identificação e classificação dos entrevistados | 26 |
| 2.3. Perguntas..... | 28 |
| 2.4. Análise dos dados..... | 28 |
| 2.5. Conteúdo..... | 29 |
| 3. A tecnologia do tema | 31 |
| 3.1. O algoritmo..... | 31 |
| 3.2. Algoritmo de aprendizado automático..... | 32 |
| 3.3. Dos dados ao conhecimento..... | 33 |
| 3.4. Aspetos relevantes da IA..... | 35 |
| 3.5. O reconhecimento facial | 38 |
| 3.6. O reconhecimento de objetos | 40 |
| 3.7. Telemóvel e Vigilância | 41 |
| 4. Principais implicações para a segurança..... | 43 |
| 4.1. A tecnologia 5G..... | 43 |
| 4.2. A mobilidade da informação..... | 44 |
| 4.3. O uso de IA na segurança – pesquisas exemplares..... | 46 |
| 4.3.1. O exemplo da Agência Europeia da Guarda de Fronteiras e Costeira | 48 |
| 4.3.2. Exemplo nos Estados Unidos da América | 50 |
| 4.3.3. Exemplo de Inglaterra | 51 |
| 5. Limites legais a imagem digital | 55 |
| 5.1. A recolha de dados digitais | 55 |
| 5.2. A prova digital | 56 |
| 5.3. Livre apreciação da prova..... | 57 |
| 5.4. A importância da prova | 58 |
| 5.5. A Jurisprudência Legalidade da Imagem Digital..... | 59 |
| 5.6. Análise do Regulamento Geral de Proteção de Dados | 61 |
| 6. Entrevistas análise e discussão dos resultados..... | 63 |
| 6.1. 1.ª Pergunta derivada | 63 |
| 6.2. 2.ª Pergunta derivada | 65 |
| 6.3. 3.ª Pergunta derivada | 67 |
| 6.4. A pergunta Central..... | 70 |

| | |
|--|-----|
| 7. Conclusões e Recomendações | 77 |
| 7.1. Conclusões | 77 |
| 7.2. Limitações | 82 |
| 7.3. Propostas para Investigações futuras..... | 82 |
| Referências..... | 85 |
| Apêndices | 97 |
| Lista de apêndices..... | 99 |
| Apêndice A | 101 |
| Apêndice B | 107 |
| Apêndice C | 113 |
| Apêndice D | 121 |
| Apêndice E | 133 |
| Apêndice F..... | 137 |

1. INTRODUÇÃO

O mundo enfrenta novos desafios de ordem, política, económica, social e ambiental, com fortes nuances em radicalização religiosa, migração em massa, ataques cibernéticos globais, terrorismo e crime organizado. A capacidade para operar neste ambiente sensível envolve os diversos atores de segurança pública, privada e o cidadão.

Objetivamente é necessário ganhar vantagem tática para mitigar estes novos desafios, usando todos os meios legais a disposição para recolher e processar dados de todas as fontes de informação relevantes para o cumprimento da missão.

Ao mesmo tempo, surgiu a internet das coisas (IoT), que são dispositivos eletrónicos de recolha de dados, tais como, telefones *smart*, relógios *smart*, câmaras digitais, etc., com diversos sensores de vigilância ligados as redes sociais, que se tornaram os maiores veículos de recolha de informações de vigilância e, impactam na forma de organizar a segurança, por diversos aspetos, tais como, a pegada digital que cada indivíduo cria.

O tema escolhido, assume destacada relevância atendendo a conjugação de vários fatores como: o crescimento populacional, a complexidade do crime, o aumento da mobilidade, o crescimento da informação, o aumento da capacidade computacional, melhores veículos de transmissão de dados e a implementação de novos pontos de recolha de imagens digitais. Estes fatores conjugados influenciam de forma direta a vida social, economia, ambiental, política e securitária.

1.1. ENQUADRAMENTO

Esta temática da “Inteligência Artificial, imagens digitais e Segurança Pública” do ponto de vista da transformação digital é revolucionário porque potencia o uso de sistemas inteligentes para transformar processos manuais e rotineiros em processos automatizados e no limite em tempo real.

A Segurança Pública (SP), é um desafio para os Estados, atendendo ao aumento da densidade populacional, aumento da mobilidade e em muitas latitudes com reflexos diretos no incremento significativo da complexidade da atividade criminosa, com grande incidência nos crimes de colarinho branco, branqueamento de capitais, tráfico de pessoas, tráfico de narcóticos e cibercrime.

A sociedade digital, desenvolveu-se como um campo de liberdade à margem do direito, no entanto, a crescente importância social, cultural e económica que rapidamente assumiu a nível mundial, fez com que o direito fosse sendo progressivamente adaptado a salvaguardar as práticas criminais de forma extremamente dissimulada em crimes como corrupção, burla eletrónica, cibercrime, branqueamento de capitais, uso abusivo de dados pessoais, etc.

Os atentados terroristas perpetrados nos Estados Unidos da América em 11 de setembro de 2001 e em Londres em 7 de julho de 2005, não foram evitados, mas, no entanto, foi possível em poucas horas após os atentados obter-se o registo identificativo dos principais suspeitos pela sua execução, através do processamento das imagens digitais, dos corredores de acesso aos aeroportos e estações de comboios, respetivamente.

Estes acontecimentos geraram de igual modo a sensação generalizada de insegurança, desencadeando a intensificação dos processos de securitização urbana, pela aplicação de táticas para atenuar o medo, desde o reforço da visibilidade policial, com forças de aspeto mais musculado, por outro lado, uma grande tendência de utilização de meios tecnológicos, em ambientes públicos e privados de sistemas de CCTV (*Closed Circuit Television*), identificação facial, leitores de impressão digital e outros dispositivos biométricos de segurança.

A envolvimento social de utilização das Tecnologias de Informação (TI), com dispositivos como telemóveis *smart* e outros dispositivos eletrónicos é uma tendência mundial na vida da esmagadora população dos países desenvolvidos, mas também, com grande profundidade e crescimento nos países subdesenvolvidos, deste modo, as TI afetam de forma direta e indireta a vida de todos, aproximando o ser humano, no limite como um ser biónico, “o futuro mais provável é o da cibernética, da simbiose entre humanos e máquinas” (Rasmus, 2017, p. 1).

Como refere Jim Al-Khalili, (2018), é importante lembrar que o conhecimento científico em si não é bom nem mau, é a forma como o usamos que importa. Assim, existe a convicção de que dentro de uma ou duas décadas teremos cidades inteligentes controladas por IA, carros sem motorista, realidade aumentada, alimentos geneticamente modificados, formas novas e mais eficientes de energia, materiais inteligentes e uma miríade de aparelhos e eletrodomésticos em rede e falando uns com os outros. Será um mundo quase irreconhecível desde o de hoje, assim como o mundo

de hoje pareceria para alguém nas décadas de 1970 e 1980. A tecnologia é o grande vetor do desenvolvimento humano desde a prensa de Guttenberg, a comunicação digital sem fios.

A adoção tecnológica marca o salto comportamental do homem, “uma coisa que podemos dizer com certeza é que as nossas vidas continuarão a ser completamente transformadas pelos avanços, na nossa compreensão de como o mundo funciona e como o controlamos” (Al-Khalili, 2018, p. 15).

Esta simbiose entre biologia humana e tecnologia eletrónica, desenvolve-se na ação dos info-incluídos pelo reforço das funções cognitivas biológicas com meios eletrónicos, seja pela utilização de um *GPS (Global Position System)* ou da *App: Waze*; consultar o banco; receber notícias eletrónicas; consultar o *Google*; comprar na *Amazon*; comunicar e partilhar conteúdos no *Whatsapp, Instagram, Tweeter*, etc. todas estas interações integram-se como fortalecimento auxiliar do conhecimento e decisão de todos os que acedem a estas fontes de processamento de dados, criando influências positivas e/ou negativas nos seus utilizadores.

Ao mesmo tempo assistimos a um crescimento das infraestruturas físicas de dados e dispositivos públicos e privados para à captação de imagens com os mais variados fins, que poderão estar alinhados para servir a construção da segurança pública, com fontes adicionais de informação, obviamente salvaguardando o preceito da privacidade.

1.2. OBJETIVOS

O principal objetivo deste estudo é contribuir para o enriquecimento do conhecimento científico nas origens de compreensão da utilização de imagens digitais processadas por IA, de forma a tornar esta tecnologia digital uma opção viável impactando no asseguramento da SP, nas lógicas social e económica, com as suas consequências éticas, políticas e democráticas.

Este estudo permite averiguar de que forma as imagens digitais, pela grandeza dos dados digitais, conjugado ao poder da IA de forma disruptiva, abrem caminho a um potencial gerador de informações com efeitos no quotidiano das pessoas e das organizações.

Ao mesmo tempo, com o desenvolvimento do rigor científico, postular o potencial da IA no enriquecimento da capacidade decisória com efeitos na prevenção, controlo, combate à violência e à criminalidade, possibilitando a promoção da capacidade operacional com a utilização racional de recursos táticos na operação da segurança no dia a dia.

A atualidade em matéria de SP, alerta-nos para a necessidade de uma visão empoderada de prevenção criminal e reação policial, sustentadas no conhecimento científico, para potenciar outras medidas policiais já implementadas, no sentido do incremento da assertividade para a mitigação das ameaças e vulnerabilidades de segurança pública.

2. METODOLOGIA DE INVESTIGAÇÃO

A natureza da temática, nasce da minha experiência profissional de 35 anos como informático, tendo desenvolvido inúmeros trabalhos de programação, que consistem basicamente em criar algoritmos, para validar, extrapolar e comparar dados, reforçados com cuidados de governança de informação, em resumo são ações básicas que potenciaram o que hoje se chama de Inteligência artificial.

O conhecimento adquirido no curso de Políticas de Segurança, junto da Universidade Lusíada, despertou em mim, a relação causa e efeito da temática deste estudo, atendendo a atualidade tecnológica que se impõe em matéria da transformação digital, que temos vindo a vivenciar ao nível social, económico, ambiental e segurança.

Destaco a segurança, atendendo a que estamos todos cada vez mais tecnológicos e esse efeito gera a chamada pegada digital, que cadaum de nós vai construindo, antevejo com relativa facilidade, o potencial da IA como auxiliar das FSS, em áreas de prevenção criminal, investigação criminal, reação policial e manutenção da ordem publica.

2.1. METODOLOGIA

O presente estudo pretende obter um conhecimento aprofundado dos efeitos da IA, em matéria de SP, como poderá contribuir para a produção de informações, o modo como estas são percecionadas pelos FSS e qual o enquadramento estratégico das mesmas. Desta forma, também é pretensão compreender em que ponto impacta nos pilares da segurança, em matéria de produção de informações de polícia, prevenção criminal, atendendo a possibilidade potencial de incrementar o policiamento preditivo.

A metodologia aplicada é o método indutivo, a investigação permitirá, seguir o problema identificado, de forma a responder ao problema de natureza científica, a fim de validar a probabilidade da sua sustentação ou a sua refuta e a partir desse ponto gerar novas hipóteses. Assim, o uso do método descritivo torna-se pertinente, visto que o mesmo serve para “identificar os principais fatores ou variáveis que existem numa dada situação ou comportamento” (Freixo, 2009, p.106).

O método científico é o que distingue o conhecimento científico, dos demais tipos de conhecimento existentes (Freixo, 2009, p. 76), baseado na observação, pretende

descrever os pontos de vista manifestados nas entrevistas realizadas durante a investigação, pois contempla vários atores relevantes da SP, que de forma direta ou indireta impactam na segurança ou na tecnologia envolvente.

A fundamentação teórica é baseada na estratégia bibliográfica, realizada em pesquisas anteriores, que sustentam a importância do tema, a partir do registo disponível, desde obras académicas, artigos científicos publicados, para se obter os dados relativos aos conceitos científicos decorrentes de investigações anteriores, como fontes analíticas de embasamento deste estudo, “os textos tornam-se fontes dos temas a serem pesquisados” (Severino, 2014, p.76).

Em complemento, aplica-se a estratégia de pesquisa documental, “como fonte de documentos no sentido amplo, ou seja, não só de documentos impressos, mas sobretudo de outros tipos de documentos, tais como jornais, fotos, filmes, gravações, documentos legais. Nestes casos, os conteúdos dos textos ainda não tiveram nenhum tratamento analítico, são ainda matéria-prima, a partir da qual o pesquisador vai desenvolver sua investigação e análise” (Severino, 2014, p.76).

O procedimento metodológico do estudo, para além de apresentar uma forte componente descritiva é, também, considerado essencialmente um desenho de investigação, que permite obter, através das respostas às questões levantadas nas entrevistas, com o objetivo de conseguir uma diminuição de riscos de erro (Freixo, 2009).

O método de investigação qualitativo, assenta em fundamentos epistemológicos, como modelo de conhecimento científico do mundo humano (Severino, 2017). A finalidade da pesquisa científica não é apenas um relatório ou descrição de fatos levantados empiricamente, mas o desenvolvimento de um carácter interpretativo (Lakatos e Marconi, 1992), no que refere ao conhecimento obtido.

2.2. IDENTIFICAÇÃO E CLASSIFICAÇÃO DOS ENTREVISTADOS

Os entrevistados são atores relevantes do sistema de SP, com preponderância direta ou indireta em setores diferenciados da atividade de SP, houve o cuidado de estabelecer um leque de sensibilidades, para obtenção da visão o mais alargada possível relativamente os matizes da temática.

Uma das técnicas de pesquisa do estudo, consiste nas entrevistas estruturadas, o pesquisador visa apreender o que os sujeitos pensam, sabem, representam, fazem e argumentam (Severino, 2014).

Tabela 1 - Entrevistados

| Nomes | Referencias |
|----------------------------------|--|
| Dr. Jose Manuel Anes | Perito superior de criminalista Professor universitário. Presidente do OSCOT- Observatório de Segurança, Criminalidade e Terrorismo. |
| Dr. Pedro Jose Lopes Clemente | Superintendente-Chefe da PSP Professor universitário. Inspetor Geral na PSP. |
| Dr. Luis Manuel André Elias | Superintendente da PSP Professor universitário. Diretor do Departamento de Operações na PSP. |
| Dr. Manuel José Serrano Faustino | Subinspetor da Polícia Marítima. Chefe de Divisão de Investigação Criminal na Polícia Marítima. |
| Dr. Paulo Alexandre Nicolau | Inspetor coordenador superior Professor universitário. Diretor regional do SEF Madeira. |
| Eng.º Bruno Tomé | 1º Sargento da GNR Engenheiro Informático Analista de Cibersegurança da GNR. |

2.3. PERGUNTAS

Deste modo, nasceram três perguntas derivadas, como sendo determinantes para a investigação da pergunta central, que orienta este estudo.

A pergunta central identificada é:

Quais são os principais contributos da Inteligência Artificial para o processamento de imagens digitais a utilizar na segurança pública?

Para balizar a pergunta central, identificou-se as seguintes perguntas derivadas:

P1: Qual a relevância da IA para a prevenção criminal e reação policial?

P2: Quais os principais contributos da IA para a gestão dos recursos policiais?

P3: Quais as principais etapas e ou tecnológicas (e.g. IA) necessárias para uma inovação na recolha de dados numa força de segurança pública?

2.4. ANÁLISE DOS DADOS

A análise compreende a identificação de todos os elementos integrantes das entrevistas, expressos de maneira explícita ou implícita, com relevância para o tema, com especial atenção a fatos históricos, acontecimentos, afirmações de fato e elementos de causa e efeito.

Outro aspeto complementar é análise das relações, com o objetivo de encontrar as principais relações e em estabelecer conexões com os diferentes elementos constitutivos do texto (Lakatos e Marconi, 1992).

A análise interpretativa regulou o processo de análise textual das entrevistas, compreendendo os elementos e as relações, destacando as evidências observadas, como interpretar, em sentido restrito, é tomar uma posição própria a respeito das ideias enunciadas, é superar a estrita mensagem do texto, é ler nas entrelinhas (Severino, 2014).

A interpretação analítica do texto, origina uma fase adicional da análise crítica, está “avaliação tem duas perspectivas: de um lado, o texto pode ser julgado levando-se em conta a sua coerência interna; de outro lado, pode ser julgado levando-se em conta a

sua originalidade, alcance, validade e a contribuição que dá à discussão do problema” (Severino, 2014, p.61).

As conclusões apuradas, refletem uma das etapas nucleares da investigação, consistindo na análise dos dados produzidos pelas entrevistas, de modo a estudar, decompor, dissecar, dividir, interpretar. A análise de um texto refere-se ao processo de conhecimento de determinada realidade e implica o exame sistemático dos elementos (Lakatos, 1992, p.23)

Assim, permite validar o quanto a argumentação é coerente com os objetivos das entrevistas e por outro lado desenvolver um juízo crítico de raciocínio, para apurar se efetivamente se “consegue uma colocação original, própria, pessoal, ... a relevância e a contribuição específica do texto para o estudo do tema” (Severino, 2014, p.61).

2.5. CONTEÚDO

A presente dissertação contém sete capítulos, de forma a permitir a apreciação estruturada dos conceitos relevantes que sustentam o estudo a volta da pergunta central.

O capítulo 1 reflete o contexto da situação securitária, a relevância do tema e aspetos de enquadramento nas novas formas de criminalidade, como o terrorismo e os efeitos da evolução tecnológica, destacando a mobilidade digital.

O capítulo 2 retrata o método científico aplicado, a motivação do tema, a descrição dos entrevistados, assim como, o método de análise das entrevistas,

O capítulo 3 introduz a base científica da descrição conceptual da IA, alguns aspetos do potencial disruptivo da sua aplicação, a sua envolvência e alguns pressupostos do conhecimento em produção.

O capítulo 4 aborda as novas tecnologias na perspetiva do seu impacto revolucionário com que nos apossaremos a comunicar, antecipando o crescimento exponencial da mobilidade digital, que se forem acautelados, abrem um manancial de possibilidades à interação social.

O capítulo 5 enumera os principais limites legais à luz das leis da República Portuguesa em matéria de tratamento de dados digitais, assim como a necessidade imperativa de

respeito pelos direitos, liberdades e garantias do cidadão, com especial destaque para o Regulamento Geral de Proteção de Dados.

O capítulo 6 descreve as manifestações colhidas através das entrevistas, permitindo apreciar a opinião de relevantes atores com influência direta ou indireta na segurança pública. Antever o enriquecimento direto do exercício da segurança pública, com a aplicação prática de inovações tecnológicas que permitirão, melhor acompanhamento das operações no terreno, bem como interação em tempo real entre os agentes da lei.

O capítulo 7 são apresentadas as conclusões da pesquisa e a resposta à questão central e algumas considerações com impacto na segurança pública. Na visão da melhoria contínua dos processos operacionais, na utilização de uma ferramenta como auxiliar da celeridade judicial, ao contribuir para uma redução temporal e assertividade na investigação criminal, tendo em vista acrescentar valor a sensação de segurança do grande público.

3. A TECNOLOGIA DO TEMA

Os sistemas de vigilância nesta fase foram baseados manualmente e utilizados para reconhecer, rastrear e identificar quaisquer objetos, diferentes tipos de infrações de segurança e violações são baseados em observações humanas, olhando para os ecrãs de monitores (Yan, 2018, p.3).

O processamento de imagens digitais consiste em utilizar a capacidade dos computadores para identificar, comparar e, projetar informações baseadas no espólio de dados disponíveis internamente nas organizações, assim como os publicados na internet. Os sistemas de vigilância orientam-se para os objetivos da transmissão em tempo real, com robustos algoritmos de visão computacional, aprendizagem automática da variabilidade da cena e padrões de comportamentos humanos, colmatando o fosso entre o mundo físico e a interpretação da linguagem natural (Yan, 2018, p.4)

A sociedade da informação reflete-se na generalizada facilidade ao acesso à informação, sendo inequívoco o crescimento do armazenamento de dados, é esperado que, na comparação com a atualidade, o mundo consuma até 20 vezes mais dados em 2030 (Grijpink *et al.*, 2020, p. 3), devido ao crescimento exponencial do volume de dados gerados através da internet, de igual modo pelas redes 5G, satélites de baixa órbita, IoT, comércio eletrónico, banca, mensagens, imagens e sistemas eletrónicos privados ou governamentais.

Esta estabelece a simbiose entre pesquisa e informação para agilizar a interação societal, nos vários serviços em que quanto mais dados, mais informação pode ser obtida, a próxima fase da resiliência digital irá estimular um maior investimento em serviços para lidar com os desafios persistentes e outros novos, relacionados às iniciativas de inteligência empresarial (Hamel *apud* Ossamu, 2021), o mais conhecimento é gerado, criando o conceito de *big data*, viabilizando o uso do algoritmo, como meio de sustentação de um tema específico.

3.1. O ALGORITMO

O algoritmo no contexto deste estudo trata-se da tradução de uma ideia ou vontade em linguagem entendível por um equipamento eletrónico com capacidade de processamento, vulgo computador.

Este quando bem otimizado é o desenho da sequência lógica da vontade expressa e repete-se de maneira infinita enquanto o sistema o estiver a usar, baseado na previsão estabelecida do momento em que é desenhado, fruto dos testes e validações essenciais para que o algoritmo possa efetivamente entrar em produção de forma confiável.

Um aspeto importante é que podem ser sempre modificados, de acordo com a vontade do seu arquiteto, normalmente tendo em vista otimizar o seu desempenho, de forma a aumentar velocidade de execução e qualidade no resultado. “Os algoritmos de pesquisa em ciência e IA têm sido continuamente desenvolvidos e refinados ao longo das últimas décadas por muitas pessoas num programa sustentado de pesquisa” (Teahan, 2010, p. 225).

Segundo Pedro Domingos (2017, p. 25), “vivemos na era dos algoritmos, sendo uma sequência de instruções que diz a um computador o que fazer, administram fábricas, comercializam e encaminham mercadorias, contabilizam os lucros e mantêm os registos de tudo isto. Se de repente todos os algoritmos deixassem de trabalhar, seria o fim do mundo como o conhecemos”.

3.2. ALGORITMO DE APRENDIZADO AUTOMÁTICO

Um princípio importante da computação tradicional é que, qualquer ação consiste numa entrada e saída de dados. “A aprendizagem automática inverte esta situação: entram os dados e o resultado desejado e sai o algoritmo que transforma os primeiros no segundo. Os algoritmos de aprendizagem são aqueles que criam outros algoritmos” (Domingos, 2017, p. 30).

Um bom exemplo da utilização de algoritmo de aprendizado automático é o que acontece quando recebemos um e-mail e este é previamente verificado pelo antivírus, para que possamos usar o e-mail de forma segura, outro exemplo acontece quando utilizamos o *Youtube* e este escolhe mostrar a publicidade que vai de encontro às nossas preferências baseadas nas nossas pesquisas anteriores.

Outra forma de ver a sua aplicação é no policiamento preditivo, segundo Pedro Domingos (2017, p. 45) “ao prever tendências de crime e ao concentrar patrulhas estrategicamente onde é mais provável que estas sejam necessárias, bem como tomando outras medidas preventivas, a força policial de uma cidade pode fazer na prática o trabalho de uma outra muito maior. Sob muitos aspetos, a aplicação da lei é

semelhante à guerra assimétrica, sendo-lhe aplicáveis muitas das mesmas técnicas de aprendizagem, quer se trate da deteção de fraudes, do desmantelamento de redes criminosas ou de simples rondas de patrulhamento”. A utilização do algoritmo baseado em dados pré-recolhidos, uma vez processados, com a identificação dos padrões de incidências de tempo e espaço, produzirá uma previsão de reincidência de ocorrências.

Para se obter o potencial de grandes volumes de dados, é imperativo considerar os metadados, que são inúteis sem a modalidade de aprendizagem profunda, como método científico que possibilita dotar os computadores de geradores de descobertas, ou seja conhecimento novo, como parte integrante das componentes de IA.

Citando Al-Khalili, (2018, p. 265), as máquinas de hoje (fazendo um milhão de bilhões de cálculos por segundo) aprendem com enormes bancos de dados contendo bilhões de itens. Esse tipo de aprendizado de máquina pode encontrar padrões, em vários níveis de detalhe, em enormes coleções de dados. Isso inclui (por exemplo) a velocidade atual e a localização de cada veículo nas estradas de uma cidade, com o estado atual de cada semáforo, ou os registos médicos de cada hospital regional ou nacional, detalhando os sintomas de cada paciente, dosagens de medicamentos e resultados. Esses sistemas de IA não são programados no sentido tradicional de Faça isso, depois faça aquilo. Em vez disso, eles consistem em redes neurais multicamadas, a saída de uma camada sendo alimentada como entrada para a próxima, os algoritmos de aprendizado automático, são um meio inovador, de os computadores processarem em paralelo, grandes volumes de dados, imitando habilidade da sinapse neural, aprendendo e relacionando os objetos e ações identificadas de configuração dinâmica.

3.3. DOS DADOS AO CONHECIMENTO

Os dados qualitativos e quantitativos em registo digital são determinantes para o desenvolvimento, a capacidade de transformar os dados em conhecimento útil, de apoio a decisão, está dependente da criação prévia as capacitações de recolha dos dados envolventes, nas mais variadas formas, sejam estas estruturados, não estruturados ou semiestruturados e das mais variadas origens, públicos, privados ou particulares.

Os dados estruturados nascem pré-organizados vulgarmente em tabelas, como se fossem fichas e que dão origem as bases de dados estruturadas, por outro lado os dados não estruturados são a panóplia de fontes de dados como e-mails, livros, registos áudio, vídeo e outros, que não estão concebidos da mesma forma ou não obedecem a

forma harmoniosa de recolha ou de formato digital, já os dados semiestruturados são a mistura dos anteriores formatos de dados.

As origens dos dados podem ser externas ou internas as organizações, as externas são aquelas que estão abertas ao grande público e as internas são de acesso restrito pois, encontram-se dentro do domínio da corporação.

Os dados externos são chamados de megadados ou *big data*, embora algumas organizações pela natureza do seu trabalho também possuem igualmente megadados, vejamos como exemplo a Google, possui megadados não pelos dados que nos disponibiliza, mas sim, pela pegada digital criada pelos seus utilizadores ao pesquisarem, publicarem, assim como, a frequência com que o fazem, etc.

As várias formas de dados depois de agrupados e ordenados podem dar origem ao nascimento de informação, que por si só, não é suficiente para se obter conhecimento.

McInerney & Day (2007) sugerem que no discurso da Gestão do Conhecimento, o termo "capital social" tornou-se importante (o termo tem origem nos escritos de Marx). "Capital social" no contexto de Gestão do Conhecimento significa o poder das relações sociais e da criatividade intelectual ("capital intelectual") para funcionar como reservas e fontes de capital. Se a história sociológica da Gestão do Conhecimento é clara, a epistemologia da Gestão do Conhecimento tem sido tudo menos clara. O problema é: como se localiza o conhecimento, as relações sociais e a criatividade intelectual dentro dos conceitos e práticas tradicionais de gestão.

O expectável na envolvência de processos de IA é criação de conhecimento útil, que pode ser visto como objetivo se efetivamente produziu o resultado esperado, ou como conhecimento subjetivo se por si só não é claro, para McInerney & Day o que estava implícito ou tácito para as pessoas ou grupos deveria tornar-se explícito, para o bem da "partilha" de informação para o aumento da produtividade e para a retenção de conhecimentos caso o indivíduo ou grupo deixasse de estar disponível. Os conhecimentos precisavam de ser formalizados, capturados e talvez até limpos, de modo a adequar-se aos modos de partilha e transferência de informação "públicas" permitidas pelas tecnologias de comunicação e informação.

O conhecimento é determinante para a inteligência, afinal sem conhecimento não se podem tomar decisões sustentadas, o conhecimento é base das relações humanas, conhecer o próximo, saber o que comunicar, como comunicar, etc.

No entanto, convém enfatizar, Bertrand Russel (1926), em como a questão de como o conhecimento deve ser definido é talvez a mais importante e difícil das três [(1) a definição de conhecimento, (2) dados, (3) métodos de inferência] com as quais trataremos. Isso pode parecer surpreendente: à primeira vista, pode-se pensar que conhecimento pode ser definido como uma crença que está de acordo com os fatos. O problema é que ninguém sabe o que é uma crença, ninguém sabe o que é um fato e ninguém sabe que tipo de acordo entre eles tornaria uma crença verdadeira (Russel, 1926).

Uma definição padrão de conhecimento, atribuída a Platão, é que existem três condições exigidas antes que um agente possa ter conhecimento é de que o conhecimento deve ser justificado, verdadeiro e acreditado.

3.4. ASPETOS RELEVANTES DA IA

A IA configura-se como a competência de processar *big data* ou sejam grandes volumes de dados (estruturados, não estruturados ou híbridos, tais como: imagens, áudio, vídeos, textos, etc.) para um determinado fim, inspirado na imitação da inteligência humana, trata-se de uma ferramenta de software, que permite a automação de tarefas, baseada no conhecimento adquirido.

De acordo com Kai-Fu Lee (2018, p. 132), estamos a viver a quarta vaga de IA, sendo a primeira originária na internet, com o seu apogeu em 2012, que se prende sobretudo com a utilização de algoritmos de IA como motores de recomendações, sistemas que aprendem as nossas preferências pessoais e depois nos apresentam conteúdos escolhidos à nossa medida.

A obtenção destes resultados como forma de conhecimento é dominada pelas empresas de internet por possuírem o maior volume de dados com os conteúdos e preferências pessoais.

A primeira vaga de IA de internet deu origem a novos negócios de publicação digital de histórias virais, identificadas por algoritmos de IA que percorrem a internet à procura de

conteúdo, utilizando processamento de linguagem natural e visão computacional para assimilarem artigos e vídeos de uma vasta rede de sites associados e fornecedores contratados. Depois, usa o comportamento passado dos seus utilizadores, os seus cliques, leituras, visualizações, comentários e por aí fora, para selecionar um fluxo de medidas feito a medida dos interesses de cada um (Lee, 2018, 132).

O surgimento da segunda vaga é voltado para a IA empresarial, pois ao contrário da primeira que necessitava de recolher os dados das preferências pessoais dos conteúdos internet, a segunda é centrada nos dados das organizações que ao longo dos anos foram registando as suas operações comerciais, financeiras, movimentação de produtos, prestação de serviços e outras que de forma estruturada, foram armazenadas em bases de dados.

Os algoritmos da segunda vaga extraem das bases de dados empresariais, correlações não visíveis ao olho humano, de comportamento, desempenho das organizações, de forma a encontrar causa e efeito para criar agilidade e melhoria do desempenho organizacional (Lee, 2018, 132).

Esta vaga despoletou novas oportunidades de negócio, pois fez nascer empresas especializadas em desenhar algoritmos, de análise de base de dados para deteção de fraudes e descobrir estrangulamentos organizacionais para a melhoria da eficiência organizacional, criando conhecimento de apoio a decisão.

A IA empresarial é de certo modo mais facilitada embora tenha a sua complexidade e carece de conhecimentos profundos para sua conceção, pois trata de analisar dados que se encontram armazenados de forma estruturada, de uma regra geral classificados e rotulados de uma forma organizada.

Para Kai-Fu Lee (2018, p. 142) as aplicações da segunda vaga de IA têm impacto imediato no mundo real, mas os algoritmos ainda continuam a lidar puramente com informação digital mediada por seres humanos. A terceira vaga de IA muda tudo isso ao dar à IA dois dos instrumentos mais valiosos na recolha de informação: *olhos e ouvidos*.

A IA com perceção nasce com à terceira vaga, até então podíamos armazenar fotos, vídeos e áudios em formato digital, mas unicamente para observação humana, não existia software capaz de entender ou identificar o seu conteúdo (Lee, 2018).

A novidade é que os algoritmos são agora capazes de “agrupar os pixéis de uma imagem digital em aglomerados com sentido e de reconhecer objetos quase da mesma forma que o nosso cérebro faz: pastor-alemão, semáforos, o nosso irmão Patrick e por aí fora. Acontece o mesmo com os dados áudio. Em lugar de armazenar apenas os ficheiros de áudio como seleções de coisas digitais, os algoritmos conseguem encontrar palavras e muitas vezes analisar o sentido de frases inteiras” (Lee, 2018, p.143), este acontecimento, passou a ser um marco revolucionário de como víamos os computadores, passando a abrir novos horizontes de geração de conhecimento.

Esta tecnologia esbateu a distância entre o plano físico e o digital, criando oportunidades como o reconhecimento facial, a capacidade de comandos de voz, para interagirmos com o Siri, a Alexia ou a Cortana, como assistentes digitais para as mais diversas utilidades, tais como efetuar uma chamada telefónica, fazer uma pesquisa na internet, por um cinema, um restaurante, um hotel, etc., assim como marcar e desmarcar a agenda, alarmes, etc.

O crescimento evolutivo tem estado a transformar a conceção e através “da digitalização do mundo irá eliminar pontos de atrito habituais e adaptar os serviços a cada individuo. A conveniência e a abundância do mundo virtual serão transportadas para a realidade do mundo físico. Não menos importante é o facto de que, ao compreenderem e preverem os hábitos de cada cliente” (Lee, 2018, p. 148), fica-se em posição para balancear a oferta em função da procura efetiva, de forma a maior racionalidade das necessidades, otimização de espaços comerciais mais à medida da procura, abrangendo locais de armazenagem em zonas de menor renda, possibilitando uma maior rentabilidade.

Outra tendência gerada pela IA, é o uso da IoT, destacando as pulseiras, pois contribuem decisivamente para convergência do mundo físico e do mundo digital, no modo permanente de contato com a pele permite recolha de diversos dados, que depois de processados, permitem a IA gerar informações em tempo real para alertar o utilizador de excessos com cuidados de saúde.

A quarta vaga é a IA autónoma, que representa a integração e o auge das três vagas procedentes, fundindo a capacidade das máquinas para otimizarem (a partir de dados extremamente complexos) com os seus novos poderes sensoriais. A combinação destes poderes super-humanos gera máquinas que não se limitam a compreender o mundo a sua volta, também lhe dá forma (Lee, 2018, p. 155). Posiciona a IA como

autênticos serviços do conhecimento novo, ao integrar *big data* e outras fontes de dados no quotidiano ao extrapolar múltiplas novas maneiras de obter informações.

Algumas repercussões práticas e visíveis socialmente são os *drones*, *UAV*, automóveis autónomos, câmaras de *CCTV* que identificam rostos, câmaras digitais que fotografam e leem matrículas de automóveis, velocidade, intensidade de tráfego, contabilizam pessoas, etc., estas aplicações robóticas autónomas são efetivas em ambientes controlados e adaptados a maximizar a segurança necessária para a sua operação.

3.5. O RECONHECIMENTO FACIAL

A tecnologia biométrica de maior impacto na atualidade é o reconhecimento facial, atendendo a que a impressão digital, a leitura das iris ou da retina, a voz e outros não são tão ágeis e dissimulados de serem recolhidos como é o reconhecimento facial, que normalmente não requer cooperação da pessoa a identificar, em oposição aos outros meios biométricos que requerem a anuência do visado.

As faces são multidimensionais, o reconhecimento facial obedece a vários processos complexos, que operam concorrentemente para classificar e determinar de forma linear rostos, começando por detetar os rostos e seguidamente o seu reconhecimento para registo primário, ou identificá-lo através de uma base de dados de rostos pré-concebida, no entanto estão dependentes de alguns fatores ambientais, como a iluminação, o ângulo de captação, a expressão facial, dependendo da pose, a maquilhagem e adornos como óculos, chapéus, envelhecimento, etc.

Ultrapassando estas condicionantes, o reconhecimento facial é a capacidade de visão por um computador e é largamente utilizado em vigilância, segurança de informação, autenticação de sistemas, para variados fins, tais como, detetar criminosos pré-registados numa base de dados, por outro lado, registar, marcar e ordenar rostos para alimentar uma base de dados.

Para Wei (2019), diferentes corpos humanos, possuem características que são mensuráveis e computáveis, como movimento labial, marcha e gestos. As características ajudam indivíduos especiais em ambientes especiais, como militares, estádios barulhentos ou locais silenciosos exigidos. A biometria possui recursos computáveis que são aplicados para encontrar a pessoa única, ou seja, a identificação. Atualmente, a maioria dos passaportes vem com informações biométricas

indispensáveis para o controlo de fronteira em aeroportos ou estações ferroviárias, o que é uma espécie de autenticação popular. Os recursos da biometria devem ser discriminativos e abrangentes no reconhecimento de padrões.

As informações biométricas de cada indivíduo, possuem um potencial enorme de aplicações de segurança, como menciona Wei (2019, p. 138), se colocarmos a biometria humana: rosto, cabelo, movimento e ações juntos, poderíamos encontrar uma pessoa procurada automaticamente na esquadra da polícia usando a biometria. No boletim de uma pessoa procurada ou nas redes sociais, normalmente as informações do suspeito são divulgadas ao público. As características do suspeito incluem gênero, idade, nacionalidade, idioma, altura, peso, cor dos olhos, cor do cabelo, comprimento do cabelo, sobrancelhas, nariz, boca, etc. Esses recursos podem ser calculados a partir de imagens e vídeos de vigilância usando os algoritmos, ... utilizando os recursos salvos numa base de dados, isso ajuda a pesquisar a pessoa procurada em aeroportos, estações ferroviárias e terminais marítimos.

Os sistemas de vigilância visual são uma realidade, os registos obtidos por eles sobre as ações físicas dos humanos, incluindo andar, correr, bater palmas ou outros gestos comportamentais, como refere Wei (2019), usam a entrada física reconhecendo o movimento do corpo ou da mão e mais tarde na identificação de gestos através de câmaras sem a necessidade de um dispositivo de entrada física.

Existem dois tipos de gestos que podem ser usados na visão computacional, um é um gesto estático, que tem as capacidades de reconhecer uma forma ou um padrão de uma mão, membro do corpo ou reconhecimento facial, os modelos são usados incluindo combinação de modelos, redes neuronais ou técnicas de reconhecimento de padrões. Outro tipo de reconhecimento de gestos é o reconhecimento dinâmico; esta é uma série de postura, sendo reconhecida ao longo de um curto período, neste tipo de reconhecimento cada moldura de vídeo compõe a postura e a sequência de quadros define o gesto para interagir com o computador, são usadas técnicas de reconhecimento dinâmico (Wei, 2019), a utilização de cada tipo é determinada pela fonte da imagem digital em apreso, para desencadear a pesquisa.

3.6. O RECONHECIMENTO DE OBJETOS

Tratando-se de objetos, a visão computacional permite de igual modo o reconhecimento por processamento de imagens digitais, seja para identificar uma paisagem, objetos em particular como armas, viaturas, motos, um capacete, ou outro objeto específico.

A complexidade do reconhecimento e classificação de objetos em imagens digitais é sustentado pelas Redes Neurais Artificiais, que processam em paralelo, enquanto trocam informações entre si sobre os padrões reconhecidos, de forma a reconhecer determinado objeto.

A deteção de objetos em movimento na vigilância visual é a etapa principal, especialmente para separação de primeiro e segundo plano. A subtração de fundo é subjetiva às mudanças de fundo e tem melhor desempenho para cada objeto em movimento, especialmente no rastreamento de objetos..., muitos locais são de interesse da alta segurança, tais como aeroportos, estações de comboio, shoppings e cruzamentos de ruas de muito congestionamento. A vigilância inteligente é benéfica a partir do reconhecimento e compreensão das ações, atividades e comportamentos dos objetos rastreados (Wei, 2019).

A evolução desta capacidade é possível através do uso de algoritmos de aprendizado, no qual um dado sistema vai evoluindo em função da qualidade dos dados utilizados no processo de aprendizagem, existem várias etapas intermédias tais como, agrupamento de pontos que constituem a imagem para separação por contorno dos diversos objetos numa dada imagem, culminando na validação do objeto no seu todo pela agregação dos vários objetos que o compõe, como exemplo um automóvel, tem rodas, portas, faróis, vidros, etc., só assim se consegue determinar efetivamente a natureza do objeto.

Outro exemplo, é o processo para “um sistema desejado de reconhecimento automático de matrícula (RAR) adota técnicas de processamento de imagem digital para localizar e reconhecer os caracteres no número da placa de matrícula do carro e produzir os resultados como uma sequência textual ou outros formatos que podem ser facilmente compreendidos na semântica. O sistema RAR tem tido várias aplicações, que requerem controlo automático da presença e identificação de um automóvel através do número da placa, tais como veículos roubados, cobrança eletrónica automática de portagens, parque de estacionamento automatizado, gestão de bilhetes de trânsito, segurança, controlo e, outros. Um sistema de reconhecimento de número de placa geralmente

consiste em cinco módulos importantes: aquisição de imagem, pré-processamento de imagem, deteção de número de placa, segmentação de imagem e reconhecimento de caracteres (Wei, 2019).

A evolução da IA no processamento de registos de vigilância visual, capacita o monitoramento de pontos de recolha de câmaras de vídeo na ordem dos milhões, ainda que tivéssemos um operador humano para cada câmara, é humanamente impossível observar e validar o conteúdo dessas imagens 24/24 horas sem recorrer a IA.

3.7. TELEMÓVEL E VIGILÂNCIA

Os telemóveis possuem uma alta taxa de penetração na vida das pessoas e que tem vindo a aumentar, atualmente veem equipados com ecrans, câmaras e microfones de excelente qualidade, com capacidade de recolha de som e imagem, por outro lado estão capacitados para conversação a distância por mensagens, voz e imagem, assim como, rodar aplicativos de navegação internet, contabilidade, vendas, banca comercial, finanças públicas, jogos, agendas, etc.

Como menciona Wei Yan (2019), a rede poderia unir forças de computação de todos os aspetos juntos. Dispositivos móveis, nuvem e redes sociais têm desempenhado papéis essenciais na vigilância inteligente moderna e irão enviar eventos de vigilância como notificações para esses dispositivos viáveis e convenientes de forma fácil.

Outro aspeto da transformação digital a considerar, tem como tendência uma maior utilização dos telemóveis sobre os computadores pessoais principalmente na camada mais jovem, atendendo a que os dados de identificação e preenchimento ou de produtos, são cada vez mais pré-existentes, faz com que seja cada vez menos necessário preencher formulários, esta tendência nasce fruto do aumento crescente da largura de banda dos dispositivos móveis.

A transformação digital, é sobre inovação e a inovação é sobre mudança, a mudança é sobre a alteração de comportamentos, tão logo surjam aplicativos em telemóveis para vigilância ou de denúncia de suspeitas de atos ilícitos, estaremos perante uma fonte de dados a escala da participação comunitária dos incumprimentos, no qual se antevê o cidadão comum no uso do seu direito de cidadania e do dever cívico de informar, a criar uma onda de envio constante de atualização de imagens e outras informações digitais

sobre os flagrantes do quotidiano, transmitindo para uma central de processamento comunitária os seus contributos de ordem social e securitária.

Assim que um serviço desta natureza seja ligado a IA, estaremos perante um potencial de informações, com alta capacidade de separar atos verdadeiros e falsos, assim como encaminhar e recomendar o seu devido tratamento. As capacidades de alerta em tempo real permitem às organizações responder proactivamente às mudanças situacionais no seu espaço social.

4. PRINCIPAIS IMPLICAÇÕES PARA A SEGURANÇA

O objetivo deste capítulo é demonstrar que estamos perante uma revolução na qualidade e capacidade das comunicações móveis, que com o surgimento da tecnologia 5G, passa a abrir novos horizontes de aplicação de tecnologias de vigilância visual, inclusive em tempo real, o 5G, combinado com o aumento da mobilidade urbana, com reflexos na mobilidade digital, são uma porta aberta ao aumento aplicativo dos dispositivos móveis para a recolha de dados utilizados na SP, seja por iniciativa do cidadão ao enviar imagens digitais para denunciar flagrantemente sociais, ou para uso dos agentes da lei em tempo real poderem partilhar com o CCC o desenvolvimento operacional no terreno.

Os sistemas de vigilância visual são constituídos por câmaras instaladas em locais remotos, identificados como locais sensíveis em áreas públicas ou privadas, de forma a transmitir imagens digitais para serem monitoradas tradicionalmente em tempo real, por operadores humanos num centro de controlo. Estes sistemas de vigilância jogam um fator importante na ajuda ao rastreamento de suspeitos de cometimento de crimes

Como conta Imed Bouchrika (2018), a utilização de tecnologias de vigilância visual deve, sem dúvidas, ajudar a diminuir os riscos e o número de crimes, servindo como uma forma de impedimento. As tecnologias biométricas podem ser um marco importante para melhorar o processo de automatização da vigilância visual, a fim de reconhecer criminosos e rastreá-los em diferentes lugares (Bouchrika, 2018).

4.1. A TECNOLOGIA 5G

O uso de TI e a sua componente de IA, passa necessariamente por existir uma infraestrutura de comunicações que tenha um custo/benefício capaz de associar valor ao resultado da operação policial, a tecnologia 5G promete a revolução esperada, como refere Konstantinos e Hamed (2016, p. 55), as comunicações futuras preveem uma infinidade de dispositivos sem fio, conectados, às vezes "inteligentes", que se comunicarão em tempo real uns com os outros. Isso é conhecido como "IoT - internet das Coisas". Esses dispositivos não serão usados apenas para interação humana, mas espera-se que haja uma procura significativa por comunicações do tipo máquina. Espera-se que o número de tais dispositivos aumente, sugerindo que haverá uma demanda cada vez maior por conexões sem fio confiáveis (Konstantinos e Hamed, 2016).

A adoção da tecnologia de comunicações 5G está a originar uma revolução no incremento imensurável da mobilidade, atendendo ao aumento da largura de banda em dispositivos moveis, o 5G é o condutor da mudança vertical na indústria da IA, IoT, Banca, robótica, comércio eletrónico, medicina, televisão, etc. Gopalaiah (2018) narra: espera-se que o 5G se estenda para além dos tradicionais serviços de voz e dados. As características da rede 5G de maior fiabilidade, menor latência, maior produção, aumento da densidade de ligação permitiriam implantações comerciais massivas de tecnologias tais como IoT, IA, RPA, AR/VR facilitando o uso de casos em indústrias como automóvel, media e entretenimento, saúde, retalho, indústria e agricultura, entre outras. Além disso, do ponto de vista social, os casos de utilização do 5G para iniciativas como as cidades inteligentes, têm o potencial de melhorar a vida dos cidadãos através de melhorias significativas em serviços como segurança pública, serviços públicos, transportes, para citar alguns.

O que representa a revolução que a tecnologia 5G oferece, é a diminuição do tempo de latência nas comunicações móveis, o que abre novos futuros ao nível da realidade virtual e aumentada, imagens 3D, imagens 4K, permitindo a aplicação prática de imagens de alta-definição em tempo real, deste modo será possível realizar intervenções cirúrgicas robotizadas a distância, partir de um local remoto.

Este cenário de comunicações sem fios, com tão baixo tempo de latência, possibilita veículos de condução autónoma, ativando a capacidade de predição e rastreamento da envolvência situacional, viabiliza um sem fim de atividades que até então só era possível por cabo físico de fibra ótica.

A capacidade de mobilidade digital será igualmente intensificada pelo aumento exponencial do número de dispositivos que podem estar ligados em simultâneo a uma dada célula de comunicações, criando deste modo benefícios para toda a cadeia de valor, desde o consumidor até as organizações, este aumento de dispositivos amplifica o crescimento do acesso a rede digital na chamada última milha, permitindo aumento da inclusão pelo nível de desempenho que possibilita.

4.2. A MOBILIDADE DA INFORMAÇÃO

Os resultados dos estudos sobre mobilidade realizado por Moura (2018), consta que ao referirem-se à mobilidade, teóricos contemporâneos (Creswell, 2014; Kaufmann, 2004; Sheller, 2011; Urry, 2006) levam em conta não apenas o movimento físico de pessoas,

informações e objetos. Eles tratam também da mobilidade virtual, imaginária e comunicativa. O conceito vem evoluindo e incorporando novos aspetos que decorrem da evolução da sociedade e das tecnologias.

Como afirma Matos (2018), observar o fenómeno do nomadismo digital pode proporcionar *insights* valiosos ..., flexível e desterritorializado, e dos impactos da condição pós-moderna no campo da produção. Tudo isso atrelado ao universo das transformações tecnológicas que, por sua vez, também alteram radicalmente o nosso universo cultural, fazendo emergir novas paisagens subjetivas como aquelas perseguidas pelos nómadas digitais.

Os telemóveis ou dispositivos móveis digitais, possuem a capacidade de emissão e receção de informação em mobilidade. O uso prático das tecnologias móveis, impõem a mobilidade digital. Como menciona Renata Motta (2009), compreende como tecnologias móveis em suas estratégias e meios que aumentem a possibilidade de se comunicar, criar, se relacionar e produzir. Num mundo ativado pelas diferentes tecnologias de informação e comunicação, a Internet e os telefones celulares ganham destaque, alcançando os mais remotos cantos do planeta. Esses dispositivos revolucionaram não apenas a maneira como trabalhamos, nos organizamos e criamos, mas carregam o potencial para mudar a forma como instituições de carácter social e cultural podem intervir nas mais diversas comunidades com suas ações sociais (Motta, 2009, p. 4).

A consequência direta da mobilidade da informação origina uma panóplia de conteúdos em que, os internautas “contribuintes comentam, codificam, encaminham, leem, assinam, conectam, moderam, fazem remixagens, compartilham, colaboram, escolhem favoritos, escrevem, trabalham jogam, conversam, fofocam, discutem e aprendem... Eles compartilham informações sobre suas músicas e clubs favoritos. Eles não ficam tímidos ao listar os livros que estão lendo e os filmes que estão assistindo. Eles detalham suas orientações sexuais e informações postais com cidade, telefone e e-mail. Eles compartilham fotos, histórico educacional e empregos” (Velásques e Carboneras, 2008, p. 9).

O desenvolvimento de TI, aplicado a computação móvel está a permitir circular, mover e emitir informação em simultâneo, num ciclo crescente de inclusão social, na esteira do fomento de mecanismos que promovam canais de comunicação com maior participação do cidadão na mobilidade digital.

4.3. O USO DE IA NA SEGURANÇA – PESQUISAS EXEMPLARES

A IA na segurança é baseada, entre outros elementos, na capacidade de análise e interpretação de grandes volumes de dados, constituindo-se um auxiliar da capacidade humana, ao sinalizar, identificar, acompanhar e alertar para eventos ou objetos que indiquem ameaças, perigos, vulnerabilidades, na vertente da prevenção, combate ao crime de forma objetiva para capacitar o reconhecimento de riscos e necessidades.

A vigilância digital é um problema de segurança de ponta e tem sido aplicada de forma inédita para monitorar e proteger nossas vidas em quase qualquer lugar. É onnipresente e prático e pode diminuir muito o trabalho humano da equipa de segurança. Com a ajuda da IA, os sistemas de vigilância têm a capacidade de concluir automaticamente tarefas como deteção de objetos, reconhecimento, rastreamento, bem como ciclo de vida de eventos, incluindo deteção de eventos, reconhecimento, pesquisa, recuperação, mineração, raciocínio, etc. (Wei, 2019).

A transformação digital das organizações é o grande catalisador do desenvolvimento alcançado pela IA, ousou superar muito do imaginário humano dos anos 80, permitindo já, a otimização do trabalho humano em tempo real, a tradução simultânea em diversas línguas, os sistemas de CCTV digital com detetor de movimentos, a identificação de objetos, o reconhecimento facial, a leitura e registo de matrículas de viaturas, alertas sobre engarrafamentos, rastreamento de movimentos de aeronaves, comboios, pessoas, cargas, etc. todas estas tarefas, com impacto direto na melhoria do trabalho do homem, permitindo-nos obter um nível alto de segurança, com o qual construímos a sociedade da credibilidade nos serviços prestados por terceiros.

A fusão da identidade física e digital é igualmente uma consequência direta do desenvolvimento alcançado pela IA, atendendo a que vivenciamos uma crescente necessidade de interagir como pessoas físicas no mundo digital e os meios primários de validação de acessos, como senhas de acesso que já não possuem a robustez de segurança no contexto evolutivo da capacidade de computação atual.

A necessidade crescente de identidade digital, está a evoluir para biometria digital, conjugada na mistura integrada das formas de autenticação em sistemas digitais, como senha, *token*, impressão digital, leitura da íris, palma da mão, nas mais diversas formas de identificação visual. He Zhang (2018) confere que a biometria é estável, única e difícil

de enganar. Devido à singularidade e estabilidade dos padrões de textura e considera a íris um dos traços biométricos mais fiáveis.

Esta tendência de identificação digital, do mesmo modo que permite efetuar pagamentos por meio de autenticação biométrica, é igualmente um meio confiável de autenticação para acesso à aplicativos que requeiram reconhecimento fidedigno do utilizador. Já Zhai, relata que a autenticação biométrica providencia maior segurança do que as senhas normais de computador que são utilizadas em aplicações como: segurança bancária, sistema de segurança informática e cartão de identidade nacional, etc.

No entanto, a maioria dos mecanismos de autenticação de telemóveis existentes apenas examinam uma única certificação no ponto de entrada e não conseguem garantir a segurança da privacidade dos utilizadores durante muito tempo, enquanto os cibercrimes se tornam cada vez mais frequentes e complexos. Já Liu, Shen e Chen destacam a abordagem cada vez mais popular é chamada *de autenticação contínua*, que verifica continuamente o utilizador enquanto o telemóvel está em uso. Pode analisar o hábito de utilização do telemóvel do utilizador e conduzir a vigilância do utilizador em segundo plano durante todo o tempo, permitindo bloquear o dispositivo sempre que não identifique o utilizador autenticado.

Os autores, Marin e Krajcikova (2016) referem, que os drones usados para fins de inteligência, produzem o que foi apelidado de “grandes dados de drones” (Ackerman 2013). Os grandes dados de drones são usados para criar sistemas de deteção de colisão, onde algoritmos podem transformar as imagens coletadas por câmaras em algo que os drones podem usar. Além do problema humano de gerenciar a enorme quantidade de dados que *Predators, Reapers, Global Hawks e Sentinels* estão a gerar (por exemplo, consulte o sistema ARGUS-IS, ou seja, o Sistema Autônomo de Imagens de Vigilância Ubíqua do Solo em Tempo Real, Limer 2013).

O estado da arte é que são já uma realidade produtos como o *BriefCam*, capacitados para análise do conteúdo de imagem digital são baseados em visão computacional e aprendizagem profunda. À medida que decorre o processamento das imagens, reconhece-se e extraem-se objetos, com informações sobre o tipo e atributos desses objetos, por exemplo, pessoas, sacos, veículos, animais, tamanho, cor, velocidade, caminho, direção, tempo de morador, e muito mais. A capacidade de extrair, isolar e diferenciar entre objetos independentes, especialmente em cenas que contenham

objetos pequenos ou distantes, má iluminação, distrações de fundo ou alta atividade, é muito difícil e constitui dos grandes desafios de visão computacional e aprendizagem profunda.

Estes produtos aplicam técnicas de supressão de ruído de forma a limitar a deteção falsa de novos objetos numa moldura, filtrando os movimentos no ambiente, como ramos, sombras, ondas e nuvens.

Na criação de processos lógicos de sequência em incidentes, por exemplo, se uma pessoa "desaparece" da imagem por um período de vários segundos, ao passar atrás de um carro ou de uma árvore, é detetado e tratado como incidente. Se a pessoa entrar e sair dos limites da imagem, pode ser tratado como incidentes de objeto separados.

A IA de 4ª vaga, aplica a fusão da aprendizagem profunda e visão computacional possibilita consultar mulheres vestidas a preto e branco, andando de bicicleta, viajando para sul a 10 Km/h estes filtros aplicados permitem visualizar todos os resultados que possam ter ocorrido durante um período de um dia inteiro em literalmente segundos, este nível de atributos, permitem em poucos segundos analisar imagens que normalmente seriam necessárias várias horas para serem visualizadas.

4.3.1. O EXEMPLO DA AGÊNCIA EUROPEIA DA GUARDA DE FRONTEIRAS E COSTEIRA

A Agência europeia responsável pelas fronteiras tem estado a desenvolver várias iniciativas de utilização de tecnologia, para identificar novas formas de controlo das fronteiras utilizando o processamento de imagens com processamento de IA.

Como relata, Marin e Krajcikova (2016), graças às tecnologias de vigilância que podem transportar, os *drones* podem contribuir para a realização dos objetivos dos controlos fronteiriços da UE, ou seja, reduzir o número de migrantes que entram ilegalmente na UE, prevenir a migração indocumentada e, assim, contribuir para a luta contra a criminalidade transfronteiriça. Os *drones* podem fornecer informações aos guardas fronteiriços presentes no terreno ou no mar e, por conseguinte, contribuir para tornar a vigilância fronteiriça uma política proactiva e não reativa.

Consultado o site do Parlamento Europeu, verifica-se que o empreiteiro de defesa Airbus foi contratado pela Agência Europeia da Guarda de Fronteiras e Costeira (Frontex), para estacionar pelo menos dois *drones* israelitas do tipo Heron 1 em Malta.

Os primeiros voos foram a 3 de maio de 2021. No concurso, a Frontex estipulou que os drones devem transportar sensores eletro-óticos e infravermelhos e um radar de abertura sintética (SAR) para vigilância que não dependa da luz do dia, e equipamentos opcionais para a posição de telemóveis e satélites. Devem também ser equipados para detetar transmissões de dispositivos de emergência instalados em coletes salva-vidas mais recentes, para facilitar o resgate marítimo (Demirei, 2021).

A Agência Europeia da Guarda de Fronteiras e Costeira (Frontex) pretende utilizar drones de longo alcance para monitorizar a zona mediterrânica e, com esse objetivo, a adjudicação de um contrato no valor de mais de 50 milhões de euros há um ano. Um ou mais drones de classe MALE (altitude média e longa duração de voo) deverão ser implantados em Malta, Itália ou Grécia, mas o sistema ainda não está operacional (Demirei, 2021).

Analisando o relatório da Comissão Europeia, refere que desta forma, a Frontex passará a ser uma "força policial de fronteira europeia" com poderes anteriormente reservados apenas para os Estados-Membros. O cerne do novo regulamento inclui a aquisição de equipamento próprio da agência. No entanto, de acordo com os planos atuais, pelo menos 6 mil milhões de euros estão reservados à Frontex no orçamento de sete anos. A intenção é que a Frontex gaste grande parte do dinheiro, mais de dois mil milhões de euros, em aeronaves, navios e veículos. Os planos de atualização incluem a estação de grandes *drones* no Mediterrâneo Central e Oriental (*European Commission*).

Por outro lado, depois de testes bem-sucedidos realizados na Grécia uma colaboração entre a Frontex e a Guarda Costeira Helénica que provou que os *Aerostats* poderiam ser utilizados para a vigilância das fronteiras marítimas, a agência decidiu lançar o projeto-piloto de vigilância marítima por *Aerostat*.

Em junho de 2019, foi lançado o *Aerostat Tethered* equipado com radar, câmara térmica e sistema automático de identificação, através da colaboração entre a Frontex e a Guarda Costeira Helénica.

O *Aerostat*, é um balão de 35 metros de comprimento, tinha monitorizado ininterruptamente o campo marítimo em tempo real, numa base de 24/7, durante 28 dias seguidos, a distância de até 1.000 metros da estação base, o que resultou como forma bem-sucedida de vigilância das fronteiras marítimas (schengenvisa.info, 2020).

As iniciativas do Frontex somam outra experiência, que foi o sistema eletro-ótico Argos II com cobertura em autonomia de até 40 km e pode detetar embarcações grandes e pequenas, em funcionamento 24/7, equipado com câmara de imagem térmica de zoom contínuo, regista imagens e transmite vídeo e dados em tempo real para estações base no terreno.

De igual modo, também foi implantada uma estação de sensores portátil na ilha de Samos. A estação tem o equipamento necessário para ajudar a comparar as capacidades operacionais e as capacidades de calibração a bordo do balão, em tempo real. O equipamento foi fornecido por Portugal através da Guarda Nacional Republicana (GNR) do seu Sistema de Vigilância Marítima (SchengenvisaInfo, 2019).

Nos últimos anos, a Frontex tem lançado várias iniciativas de processamento de imagem digital, em forma de vários programas, esquemas e operações, num acumular de experiências para encontrar novas formas de reforçar a segurança nas fronteiras da UE no Espaço Schengen.

4.3.2. EXEMPLO NOS ESTADOS UNIDOS DA AMÉRICA

Tabela 2 - Resumo Compton

Em 2014, os residentes de Compton, Califórnia, descobriram que a sua cidade havia sido sujeita a um experimento de 2012 em monitoramento total de vídeo, 2 anos atrás. O Departamento do Xerife do Condado de LA contratou uma empresa de vigilância privada para testar uma câmara aérea que monitorava “toda a cidade 24 horas por dia usando vídeo de alta resolução de tudo o que aconteceu dentro do município de 10 milhas quadradas” (Friedersdorf 2014). Por 48 h, tudo na cidade foi rastreado.

Como disse o consultor de privacidade da cidade, nós literalmente assistimos Compton durante o tempo em que estávamos a voar, então podíamos dar um zoom em qualquer lugar dentro da cidade de Compton e seguir carros e ver as pessoas (Friedersdorf 2014). As imagens foram arquivadas para que, se um crime tivesse sido denunciado durante esse período, a polícia pudesse voltar e recuperar o vídeo e dar um zoom no local do crime. A demonstração vislumbrou a possibilidade de monitoramento e arquivamento abrangentes em tempo real: o redobramento digital de espaço e tempo que tornaria possível reconstruir o passado e, por meio do poder da análise de dados prever ameaças futuras. O crescente interesse no chamado policiamento preditivo depende dessa possibilidade, quanto mais dados podem ser arrecadados, maior será o alcance e o poder dos algoritmos que podem ser usados

para alocar preventivamente o poder de policiamento (c.f. McCue 2006). O reino da segurança é o habitat nativo do drone, com sua proveniência militar, a sua estratégia de assimetria e a sua ligação direta com a tecnologia de vigilância.

O experimento Compton ilustrou o impulso em direção à “onisciência diacrônica” (Parks 2001) que caracteriza a lógica dos drones. A fantasia do *drone* é cobrir todos os espaços o tempo todo: daí, a direção em direção a câmaras de alta resolução com faixas mais amplas de campo carregadas por dispositivos que podem permanecer no ar o maior tempo possível.

Fonte: Andrejevic, 2016, p. 27

4.3.3. EXEMPLO DE INGLATERRA

Citando a Stuart O’Brien (2020), o Reino Unido é uma das nações mais vigiadas do mundo, calcula-se em 5.9 milhões de câmaras, dos quais 96% de propriedade privada, aproximadamente 691.000 instaladas somente na cidade de Londres.

Refere que a taxa de sucesso de resolução de crimes por consulta as imagens criam uma correlação positiva, entre a presença de câmaras e crimes resolvidos com sucesso. “O desenvolvimento de CCTV foi visto por muitos como um grande avanço na prevenção criminal”.

Um dos grandes constrangimentos, são aos milhares de horas despendidas, a analisar um grande número de câmaras, a procura de um pormenor relacionado com o crime em pesquisa.

A vigilância em tempo real vai testar a tolerância britânica para as câmaras, a tecnologia de reconhecimento facial está a escrutinar-se num país mais habituado à vigilância.

Um episódio de vigilância policial possibilitou em Cardiff, País de Gales, algumas horas antes de um recente jogo de rãguebi, entre multidões de fãs vestidos com cores de equipa de vermelho e verde, e comerciantes de calçada a vender cachecóis e bandeiras, agentes da polícia saltaram de uma carrinha branca.

Os agentes detiveram um homem que transportava um grande café Starbucks, fizeram-lhe uma série de perguntas e prenderam-no. Uma câmara ligada à carrinha tinha

capturado a sua imagem, e a tecnologia de reconhecimento facial usada pela cidade identificou-o como alguém procurado por suspeita de agressão.

A Grã-Bretanha tradicionalmente sacrificou a privacidade mais do que outras democracias ocidentais, principalmente em nome da segurança. O uso pelo governo de milhares de câmaras de circuito fechado e a sua capacidade de monitorizar as comunicações digitais têm sido influenciados por bombardeamentos domésticos durante anos de conflitos envolvendo a Irlanda do Norte e ataques desde 11 de Setembro de 2001 (Satariano, 2019).

Existem já no mercado de software, produtos que permitem tratar várias fontes de imagens digitais, vou referir a experiência do produto *BriefCam*, que se destaca pela capacidade de classificar os vários tipos de objetos visuais por cores, tamanhos e características específicas.

Tabela 3 - Resumo *BriefCam*

"Posso dizer com 100% de convicção que o *BriefCam* nos permite procurar e encontrar provas que não poderíamos ter encontrado antes. Usamos este sistema pelo menos duas vezes por dia, cerca de 700 ou 800 vezes por ano." (Sargento Johnmichael O'Hare do Departamento de Polícia de Hartford).

Proteger 125.000 residentes e impulsionar o crescimento económico, o Departamento de Polícia de Hartford (HPD) tem um desafio vasto e difícil que é comum a todas as cidades. Deve proteger os cerca de 125.000 residentes da cidade e as inúmeras empresas, enquanto desenvolve estratégias para diminuir a criminalidade. No entanto, a Polícia de Hartford vê o seu papel como mais do que apenas proteger os residentes de Hartford, o HPD está a esforçar-se para revitalizar a cidade e impulsionar o crescimento económico, transformando Hartford numa cidade que atrai visitantes e novos negócios.

Para promover estes objetivos, o HPD criou o Centro de Crime em Tempo Real que inclui um sistema FluidMesh sem fios que permite que as câmaras de videovigilância da HPD sejam colocadas em qualquer lugar da cidade. A implantação de um sistema de vigilância deste tamanho exigiria geralmente 30 novos oficiais para rever e reagir às filmagens em tempo útil. O departamento de Polícia de Hartford precisava de uma solução que lhe permitisse rever e pesquisar rapidamente volumes maciços de vídeo, e transformá-lo numa fonte de inteligência acionável, a *BriefCam* foi a escolhida para resolver este desafio.

Multiplicar a força policial, a HPD usa o BriefCam para agilizar as operações de várias maneiras, desde rastrear e identificar suspeitos até à prevenção proativa da criminalidade.

Ao usar a funcionalidade de vigilância do mapa de calor para identificar pontos quentes do crime, por exemplo, os oficiais rastreiam os níveis de atividade e criam planos de ação estratégicos em áreas suspeitas de distribuição de drogas. Antes do BriefCam, um detetive disfarçado dormia à porta de uma casa de droga suspeita ou local de distribuição. Agora, as câmaras secretas são montadas discretamente e usando a tecnologia de Deep Learning e Synopsis da BriefCam permitindo que um detetive possa pesquisar horas de vídeo em minutos e confirmar rapidamente se as drogas estão a ser distribuídas a partir deste local. A polícia de Hartford pode agora vigiar 6 a 10 locais usando as mesmas horas de detetive que anteriormente exigia para uma única vigilância. Nos casos em que a polícia não tenha câmaras num determinado local, a BriefCam também pode carregar e analisar rapidamente vídeos externos de outras fontes para apoiar a investigação.

Resolução de crimes anteriormente insolúveis, a polícia de Hartford está a usar o BriefCam para resolver crimes que anteriormente não conseguia resolver. Depois de um tiroteio fatal numa discoteca, a única pista foi a descrição das testemunhas do suspeito e do veículo. Com o BriefCam, a Polícia procurou dias de vídeo antes do incidente para identificar veículos semelhantes e, em seguida, fazer zoom para ver a cara do condutor. Combinaram com o suspeito e o veículo, usando um vídeo que foi tirado num sinal vermelho horas antes do crime. Com base nesta informação, a polícia conseguiu um mandado de busca, esfregou o suspeito para o ADN, e confirmou uma correspondência de ADN com provas da cena do crime. Sem a capacidade de procurar rapidamente dias de filmagens de várias câmaras próximas, este suspeito pode não teria sido apanhado.

Fácil integração e preparação, a parceria da BriefCam com as principais empresas de VMS cria integrações perfeitas que poupam tempo. Quando a HPD pesquisa e faz comentários em BriefCam, os marcadores são automaticamente transferidos para o seu Milestone VMS. Com um clique, o PD de Hartford pode ver o mesmo ponto marcado no Milestone VMS e preparar provas para o tribunal.

Esta simples interação elimina a necessidade de carregar e descarregar informações entre o BriefCam e o VMS, e torna a força policial mais produtiva.

Uma visão para o futuro, o HPD vê um potencial incrível para como o BriefCam pode revitalizar uma cidade aproveitando o poder do vídeo para um planeamento inteligente e proativo. "O vídeo é o último ativo subutilizado", afirmou O'Hare. "Com o BriefCam podemos procurar pessoas e objetos usando critérios específicos. Reduz o que costumava durar horas de pesquisa manual até apenas minutos. Ajuda-nos a ser mais eficientes e eficazes na captura

de criminosos. Mas é mais do que reduzir o crime; trata-se de planejar percursos pedestres e de bicicleta para aumentar a segurança, e rastrear padrões de tráfego para encontrar os melhores locais para eventos, restaurantes e lojas de retalho. O BriefCam está a ajudar-nos a combinar segurança com uma abordagem inteligente ao planeamento da cidade. É mudança de condução para que os visitantes não cheguem a um evento em Hartford e se retirem em seguida. Eles ficam, jantam, gastam dinheiro e revitalizam a cidade."

Fonte: www.BriefCam.com

O atual nível de desenvolvimento das infraestruturas de comunicações, em termos de redes de fibra ótica, potenciadas pelo 5G, abrem um caminho de oportunidades para o uso de transmissão de imagens digitais, atendendo a que, pelo tamanho das imagens digitais estas necessitam de consumir grandes recursos de largura de banda para poderem ser transmitidas até uma central de processamento.

As experiências, identificadas neste capítulo são um subproduto do desenvolvimento das vias de comunicação digitais no presente e da capacidade de os sistemas processarem algoritmos, com imagens distinguindo os diversos objetos inerentes, tais como rostos, matrículas de veículos e diversos objetos (roupas, locais, sinais particulares).

A capacidade de aprendizagem profunda da IA é o vetor que possibilita aos sistemas lidar evolutivamente com a panóplia de objetos capturados em matriz digital e separá-los de forma a ser serem perceptíveis pela compreensão humana, para que possamos classificá-los como pessoas, carros, etc.

A tecnologia vem sendo um auxiliar do desempenho do homem, tornando-a cada vez mais capaz, em termos de prevenção criminal e investigação criminal, podemos classificar o uso de IA como uma ferramenta de ajuda a indiciar a localização e a caracterização de presumíveis participantes num local de crime, atendendo a capacidade da IA, de procurar para separar no espólio de imagens digitais a partir de uma fonte legal, os seus presumíveis elementos que caracterizaram um dado evento, a fim de servir como guia a investigação policial.

5. LIMITES LEGAIS A IMAGEM DIGITAL

Este capítulo pretende enquadrar, os principais limites legais à luz das leis da República Portuguesa em matéria de tratamento de dados digitais, logo, observando o Regulamento Geral de Proteção de Dados, na forma como trata o respeito constitucional pelos direitos, liberdades e garantias do cidadão.

5.1. A RECOLHA DE DADOS DIGITAIS

A recolha de imagens por indivíduos particulares é permitida desde que não sejam para um fim ilícito, tal como a recolha por sistemas de CCTV, assim como a recolha utilizando um telemóvel ou câmara de filmar, já os órgãos judiciais necessitam de pedido prévio e formal a Comissão nacional de proteção de dados (CNPD), sempre que necessitem de objetivamente recolher imagens.

Dentro dos caminhos legais de recolha de imagens, tais como imagens internas de um espaço empresarial, residências, de igual modo a recolha voluntaria por cidadãos na via pública, ou ainda por outro lado, a recolha profissional por órgãos de informação noticiosos, todas as diversas fontes civis de obtenção de imagens, podem pontualmente participar em denúncias particulares aos órgãos de justiça.

Todas estas fontes de registo da realidade, tornam-se relevantes numa perspetiva quantitativa, no entanto é por demais importante avaliar se efetivamente reúnem características complementares, em matéria de valor, como expõe Rosangela Marquesone (2017, 16), “a grande mudança esta no valor que se consegue obter a partir do volume, variedade e velocidade de dados, ou seja, uma mudança qualitativa”.

As características complementares obrigam a fratura de paradigmas, precisamos lidar com novos tamanhos de dados, novas velocidades, novas tecnologias e novos métodos de análise de dados (Marquesone, 2017), os seus atributos qualitativos podem ser complementados com valor e veracidade.

O valor varia em função do alcance que se pode obter pela análise dos dados que constituem as imagens, atendendo a que podem indiciar de forma direta no quesito da sua denuncia primaria, mas também, de forma indireta nos quesitos de outras denúncias em investigação, numa relação de lugar, forma, género, padrão, etc.

Já a veracidade das imagens, está relacionado com à confiabilidade dos dados (Marquesone, 2017), em pressupostos como autenticidade e legitimidade, dentro da diversidade, formatos e a ação dos agentes geradores dessas imagens.

5.2. A PROVA DIGITAL

A recolha, gravação e utilização da imagem digital esta regulamentada por lei, é importante o enquadramento legal para demonstrar as nuances a aplicação da lei relativa a este elemento de prova, atendendo tratar-se de um elemento novo, uma vez que os dispositivos de processamento digital são comumente utilizados desde os anos 70, inicialmente na Banca, processamento de salários, controlo de stocks, cálculo de estruturas e contabilidade.

A garantia dos direitos fundamentais obriga a que a prova digital enquanto elemento de obtenção de prova, seja capaz de preservar os direitos, liberdades e garantias dos cidadãos e ao mesmo tempo agilizar o uso da prova digital nos domínios da investigação criminal, para investigar e recolher meios de prova.

A obtenção da prova digital para a descoberta da verdade material em determinados crimes, é uma ferramenta insubstituível para a resolução de casos que, de outra maneira, não se solucionariam, tais como corrupção, branqueamento de capitais, ciberterrorismo, pedofilia, atropelamento e fuga, colisões entre veículos, assaltos, etc.

Fruto da problemática da evolução da aplicação de meios de processamento digital, nasceu a necessidade de instrumentos específicos na missão de suprir necessidades judiciais, trazidas à luz no curto espaço de algumas décadas, à emergência e triunfo de direitos como a palavra, a imagem, a autodeterminação informacional, a identidade genética, a integridade dos dados, proteção de dados e confidencialidade dos sistemas informáticos.

Para perseguir estas práticas criminais, aplica-se o papel da “investigação criminal, no qual compreende o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher provas, no âmbito do processo” (Portugal. leis, decretos, etc., 2021, art. 1), esta ação subordinada aos direitos fundamentais, obriga a que a prova digital enquanto elemento de obtenção de prova, seja capaz de preservar os direitos, liberdades e garantias dos cidadãos e ao mesmo tempo agilizar o uso da

prova digital nos domínios da investigação criminal, para investigar e recolher meios de prova.

O destaque resume-se ao fato da imaterialidade da prova digital em oposição a prova material palpável com aspeto físico, assim sendo, a prova digital aparenta, deter um potencial acrescido para ferir direitos, liberdades e garantias que o nosso ordenamento jurídico constitucionalmente consagra e cuja proteção ali acautela. Estou em crer que, ao fazer-se uso da prova digital como meio essencial de provar para certa verdade, caminhamos na tão ténue fronteira com o risco imenso de ferir direitos fundamentais atendendo as características da prova em si.

E não obstante a prova digital possa ser fulcral para desvendar a verdade por trás de número crescente de crimes, é o também que se advirta firmemente que a mesma pode consubstanciar um perigo quando os limites às suas obtenções não estejam claríssimos e não seja o mesmo, objeto de um controlo rigoroso, seja em razão da sua natureza, da forma como se apresenta ou do método de se apreender.

5.3. LIVRE APRECIÇÃO DA PROVA

O princípio da livre apreciação da prova, diz-nos no art.º 127.º do CPP, que “salvo quando a lei dispuser de forma diferente, a prova é apreciada segundo as regras da experiência e a livre convicção da entidade competente”. Significa que, se a lei for omissa, ou por outro lado, não especificar que valor probatório tem determinada prova, o julgador decide em cada caso, segundo a sua consciência.

“A valoração da prova demonstra uma dinâmica axiológica a cargo do próprio julgador, sem que este esteja vinculado a critérios fixados na lei, de cuja conjugação no sistema da prova legal, resultaria do acerto decisório” (Neves, 2011, p. 57).

Através de Figueiredo Dias, “A liberdade de apreciação da prova é, no fundo, uma liberdade de acordo com um dever, o dever de perseguir a chamada «verdade material» -, de tal sorte que a apreciação há-de ser, em concreto, reconduzível a critérios objetivos e, portanto, em geral suscetível de motivação e de controlo (possa a lei renunciar à motivação e ao controlo efetivo)” (Dias, 1974, p. 202-203)

Ainda que seja esta uma matéria de controvérsia tendo em conta a subjetividade que está patente na valoração que o juiz dá a determinada prova, certo é, que é necessária

uma convicção absoluta, relativamente à veracidade da prova apresentada, para que o julgador a aprecie, atribuindo-lhe um peso decisório no processo. Quando assim não sucede, deve o julgador saber agilizar estas suas indeterminações, com o *Princípio in dúbio pro reo*.

5.4. A IMPORTÂNCIA DA PROVA

Na atualidade, o preceito da investigação criminal obedece ao conceito das proibições das provas, como uma das instituições mais marcantes do novo ordenamento processual, erigido dos alicerces sediados diretamente na Constituição da República Portuguesa de 1976 (Andrade, 2006), trata-se de um dos meios da lei proteger os cidadãos contra as ingerências abusivas dos seus direitos (Silva, 2013).

A Constituição da República de Portugal refere no seu art.º 32.º, n.8 “São nulas as provas obtidas mediante tortura, coação, ofensa da integridade física ou moral da pessoa, abusiva intromissão na vida privada, no domicílio, na correspondência ou nas telecomunicações”. Deste modo o legislador demarcou a expressão positiva e explícita ao conceito e ao regime das proibições de prova (Andrade, 2006).

O regime da proibição de provas funciona como um limite a descoberta da verdade material, que se sobrepõem aos interesses públicos de perseguição penal, de forma a não ferir outra lei da Constituição no seu art.1º na defesa da dignidade humana, como “matriz material e última do direito das proibições de prova” (Canotilho, Moreira, 2006, p. 525).

Os aspetos das nulidades processuais e as proibições de prova são tratados de forma distinta no CPP nos seus artigos 118.º, 125.º “legalidade da prova” e 126.º “o princípio da legalidade das nulidades”, pelo que, no art.º 125.º refere a todos os meios de prova admitidos em direito desde que não sejam proibidos por lei (Silva, 2008), aqui cabem todos os meios de prova que forem proibidos por lei, incluindo os atípicos, já o art.118.º nº2, clarifica que se “a lei não cominar a nulidade, o ato é irregular” e no art.118.º nº3, estabelece-se a fronteira entre as nulidades e as proibições, referindo que “as disposições do presente título não prejudicam as normas deste Código relativas à proibições de prova” e por último o art.126.º encerra em si tanto o conceito de proibição de produção da prova, como de proibição da sua valoração, como sendo verdadeiras limitações a descoberta da verdade material e que carregam como efeito a nulidade do

ato proibido, pelo que tudo se há de passar como se a prova não existisse (Jesus, 2015), deste modo não se podem usar provas obtidas a margem da lei por serem nulas.

Exemplificando isso acontece quando se obtêm as provas sem autorização do Juiz de Instrução Criminal (JIC), tais como escutas telefónicas, recolha de imagens, apreensão de correspondência, confissão extorquida, no qual a confissão de onde encontrar o produto do crime, que acaba por ser apreendido a posterior, no entanto em qualquer um destes casos, atendendo a que são procedidas de ilegalidade, a prova ilícita terá de ser considerada nula.

Outro aspeto relevante sobre as provas prende-se com as provas secundárias geradas pela prova ilícita ou não aceite no processo, atendendo a que uma prova gerada a partir de uma violação, inquina as provas obtidas subsequentemente por terem sido produzidas com vício e assim garantir que determinado meio de prova considerado proibido não possa, em hipótese alguma, ser utilizado.

5.5. A JURISPRUDÊNCIA LEGALIDADE DA IMAGEM DIGITAL

A jurisprudência posiciona-se como farol decisório da conduta para a validação da necessidade objetiva da recolha de imagens, desde que a sua motivação não seja um propósito ilícito, mas sim a procura pela verdade material no direito de defesa do prejudicado.

Veja-se a síntese de acórdãos relevantes dos Tribunais:

- O acórdão do T.R.G., proc. n.º 102/09.8GEBRG.G2, de 29/04/2014: “O direito à imagem está tutelado criminalmente, mas apenas na medida em que não esteja coberto por uma causa de justificação da ilicitude. Não constituem provas ilegais, podendo ser valoradas pelo tribunal, a gravação de imagens por particulares em locais públicos, ou acessíveis ao público, nem os fotogramas oriundos dessas gravações, se se destinarem a documentar uma infração criminal e não apresentarem «*núcleo duro da vida privada*» da pessoa visionada (onde se inclui a intimidade, a sexualidade, a saúde e a vida particular e familiar mais restrita)”.
- Acórdão da Relação de Coimbra de 20 de setembro de 2017 em processo penal é permitida a utilização de imagens previamente obtidas através de um sistema de videovigilância de um estabelecimento comercial. Tais imagens não

respeitam ao “núcleo duro da vida privada” das pessoas visionadas e existe justa causa (prova de uma infração criminal), razão pela qual não se trata de método proibido de prova (ainda que, porventura, não tenha sido obtida autorização da CNPD para a instalação do sistema de recolha de imagens).

- Acórdão da Relação de Lisboa de 10 de maio de 2016 Imagens captadas em local de acesso público, mesmo sem o de consentimento do visado, não correspondem a qualquer método proibido de prova, por não violarem o núcleo duro da vida privada, avaliado numa ideia de proporcionalidade e por existir uma justa causa na sua obtenção e utilização, que é a prova de uma infração criminal. A falta de parecer prévio favorável da CNPD, só por si só, não torna a gravação ilícita, nos termos da lei penal.
- Acórdão da Relação de Évora de 29 de março de 2016, é, em princípio, admissível a valoração das fotografias ou filmes que não tenham sido obtidos de forma penalmente ilícita. Filmar a materialidade de autoria de um crime e de utilizar posteriormente o vídeo como prova do facto, embora possa eventualmente preencher a factualidade típica do crime de gravações e fotografias ilícitas (Artigo 199º da nota prática nº 12/2017 - jurisprudência sobre prova digital 14 Código Penal), pode ser lícito, por exemplo, se quem filmou agiu ao abrigo do direito de necessidade (Artigo 34º do Código Penal), o que vale tanto para a obtenção do vídeo como para a sua posterior utilização em processo crime, pois esta utilização constitui a concretização daquele mesmo fim.
- Acórdão da Relação de Lisboa de 14 de maio de 2009 Apesar de o Artigo 199º, nº4, do Código Penal proibir e punir a recolha de imagens, por fotografia ou por filmagem, este direito apenas é reconhecido a quem pode legitimamente ostentá-lo e defendê-lo; não é o caso de quem entra num espaço vedado e não livremente acessível ao público e dali retira e faz seus bens que sabe não lhe pertencerem - neste caso, são lícitas e válidas como prova as imagens obtidas por câmara de videovigilância oculta.
- Acórdão da Relação de Évora de 28 de junho de 2011 A obtenção das imagens através de sistema, tendo em vista a identificação de autores de crimes, visa documentar infrações e não diz respeito ao «núcleo duro da vida privada» da pessoa visionada; é um meio necessário e apto ao exercício do direito de defesa,

pelo que está excluída a ilicitude do mesmo. Não constitui um método proibido de prova, dado que existe uma causa de justificação para a sua obtenção.

As citações síntese dos acórdãos elencados constituem a visão plena jurisprudencial ou doutrinária em conjugação com a lei no respeito dos demais interesses constitucionalmente protegidos, a bem dos direitos fundamentais dos cidadãos.

A descoberta da verdade não pode ser a qualquer preço, deve ser instruída salvaguardando o direito da dignidade humana, assim como ao direito à privacidade, os meios de prova obtidos a margem da lei, constitui a inutilização absoluta dos meios de prova.

Citando Figueiredo Dias no qual “o próprio pensamento filosófico mais recente veio mostrar que toda a verdade autêntica passa pela liberdade da pessoa, pelo que a sua obtenção a custa da dignidade do homem é impensável” (Dias, 1974, p.194).

5.6. ANÁLISE DO REGULAMENTO GERAL DE PROTEÇÃO DE DADOS

O conceito de privacidade como direito fundamental é o elemento central da Regulamento Geral de Proteção de Dados (RGPD), atendendo a que a informação é um bem precioso e necessita de ser protegido, mormente impactado pela crescente mobilidade digital, no qual a troca de informação é implícita nas redes digitais, assim como quando manifestamos as nossas escolhas ao ver um filme, visitar uma página de produtos, ler uma publicação digital, etc. os provedores desses serviços registam as nossas opções e posteriormente, estas podem ser usadas para prever os nossos hábitos de consumo, ou até para vender essa informação a terceiros.

A sociedade da informação fomenta a recolha e tratamento de dados, porém os limites de recolha e manuseamento de dados passam a estar regulados pelo RGPD, que se enquadra dentro das políticas públicas na área da segurança.

O acesso aos dados rege-se pelo princípio da necessidade de conhecer a informação, devendo o tratamento ser realizado por profissional obrigado a sigilo ou sujeito a dever de confidencialidade. Por outro lado, estabelece-se que os dados relativos a auxiliar na procura da verdade material, seja em processo de investigação criminal, ou na prevenção criminal, estes podem ser organizados em bases de dados ou registos

centralizados assentes em plataformas únicas que preencham os requisitos de segurança e de inviolabilidade previstos no RGPD.

As imagens gravadas e outros dados pessoais registados através de sistemas de vídeo ou outros meios tecnológicos de vigilância à distância apenas podem ser utilizados no âmbito do processo penal e nos termos do artigo 20.º do Código do Trabalho. A Lei 58/2019 estabelece limites adicionais ao referido tratamento nos n.ºs 2 e 3 do citado artigo 19.º. A título exemplificativo, elenca-se a proibição de as câmaras incidirem sobre (i) vias públicas, (ii) zona de digitação de códigos de caixas multibanco, (iii) o interior de áreas reservadas a clientes ou utentes onde deva ser respeitada a privacidade (e.g., instalações sanitárias) e (iv) o interior de áreas reservadas aos trabalhadores, bem como a exigência de, nos estabelecimentos de ensino, as câmaras apenas poderem incidir sobre os perímetros externos, locais de acesso ou sobre espaços cujos bens e equipamentos requeiram especial proteção, tais como laboratórios ou salas de informática

Outro aspeto importante é tratado no n.º 4 do artigo 19.º da Lei 58/2019 estabelece ainda a proibição genérica da captação de som pelas câmaras de videovigilância, “exceto no período em que as instalações vigiadas estejam encerradas ou mediante autorização prévia da CNPD”, sendo esta a única situação em que a Lei 58/2019 sujeita a utilização de sistemas de videovigilância ao controlo prévio por parte da CNPD.

A desaplicação pela CNPD de um conjunto muito relevante de normas constantes da Lei 58/2019, incluindo no que se refere ao regime sancionador previsto na mesma e à norma geral de desaplicação das disposições nacionais que preveem a obrigatoriedade de notificação e/ou obtenção de autorização pela CNPD para a realização de operações de tratamento.

6. ENTREVISTAS ANALISE E DISCUSSÃO DOS RESULTADOS

As entrevistas realizadas englobam profissionais relevantes da SP, com experiência de atuação, em diferentes momentos da carreira profissional, nas camadas, operacional, tática e estratégica, como modelo de entrevista foi utilizado um roteiro semiestruturado cujas questões foram referidas no item 2.4. Na elaboração do roteiro de entrevista priorizaram-se questões do tipo abertas de livre descrição.

Este capítulo expõe a transcrição parcial das entrevistas, nos aspetos relevantes para o tema, na técnica de análise interpretativa de conteúdo, apresenta-se estruturado de modo a exibir a análise qualitativa das entrevistas.

No entanto, os teores completos das entrevistas encontram-se como anexo a esta pesquisa.

6.1. 1.ª PERGUNTA DERIVADA

Qual a relevância da IA para a prevenção criminal e reação policial?

A razão da 1ª pergunta derivada (PD) é identificar, se existe visão, os desafios, a necessidade latente para abertura a mudança e concomitantemente a abrangência do processo inovativo.

Os entrevistados mencionaram o positivismo que pode originar um sistema de informações mais consistente, como refere Manuel Anes ser “Indispensável, é evidente que necessitamos no âmbito da segurança, possuir meios que nos auxiliem a perscrutar de maneira mais eficaz, por exemplo a identificação de pessoas, a identificação de atividades criminais, a prevenção de atividades criminais, por aquilo que me é dado a saber a Inteligência Artificial é um passo em frente para nos ajudar a resolver estes problemas de forma rápida”.

De igual modo Luís Elias salienta, que “há aqui diversas mais-valias que permitirão maior imediatismo na análise da informação e respostas mais rápidas, de forma a ganhar eficiência e a eficácia”, uma das mais-valias é que o uso de IA é condicionado pela necessidade de grande volume de dados de base, no qual já existe um “grande repositório de informação, que vem sendo alimentado a cerca de duas décadas”.

Outro aspeto relevante é a capacidade de aumentar o horizonte de apreciação judicial, citando Pedro Clemente “muitas vezes quando são decididas as medidas de coação aplicadas, nomeadamente a prisão preventiva ou não, é muito importante, enfim incorporar toda essa informação, de forma que a magistratura possa tomar a sua decisão”.

Pedro Clemente evidencia que “a informação hoje em dia é muito importante, a investigação criminal baseia-se sobretudo em informação, o que pressupõe dados trabalhados”, no entanto um dos desafios passa por aprimorar os sistemas a atualidade, como refere Bruno Tome “convinha também ter um sistema, que se fosse atualizando e tivesse um enquadramento legal, porque, muitas vezes ele foi desenvolvido há a muitos anos e nunca acompanhou a evolução tanto a nível criminal de procedimentos, como a nível legal e muitas vezes, o que está lá não corresponde a realidade do que está a ser feito”.

Foi expressa a importância de partilha simplificada de informação, como referiu Manuel Faustino no qual “A informação centralizada em cada OPC, pode gerar informação especulativa, muitas vezes por questões culturais, o próprio órgão não a disponibiliza em tempo real, o ideal quando se fala em informação centralizada seria um sistema único para todas as polícias”.

Esta igualmente reconhecido que existe a possibilidade de auxílio assertivo a tarefa de quem esta no terreno, atendendo as limitações de conhecimento do ser humano, como relata Bruno Tome, pois o operacional “toma conta de diversos assuntos, tanto a violência doméstica, um furto, um roubo, um acidente rodoviário, ou um assalto a mão armada, por exemplo, coação e muitas vezes uma pessoa sai de uma situação e vai para outra e se tiver algo que o ajude, que o apoie, torna-se tudo muito mais fácil, porque, é um leque tão grande, que quem está fora tem de saber, a nível criminal, de leis, de procedimentos, se tiver uma informação algo que o ajude, neste caso tem aqui estes tópicos e é assim que se deve atuar, e deve-se guardar ou salvaguardar esta prova para ser legal ao nível do tribunal judicial.

6.2. 2.^a PERGUNTA DERIVADA

Quais os principais contributos da IA para a gestão dos recursos policiais?

A entendimento da 2^a PD é nomear formas de superioridade e auxílio, na emprego e distribuição dos recursos policiais.

O crescimento da comunicação em tempo real, abre uma janela de oportunidades como refere Manuel Faustino no qual “a gestão dos recursos utilizando IA, permite-nos disponibilizar os meios necessários para cada momento real, porque temos informação presencial, é possível hoje em dia que alguém que esteja no centro de comando e controlo (CCC), numa situação de risco, por exemplo um evento desportivo, um incidente num transporte público, seja o tipo de ação que for, mesmo a mais violenta, é possível alguém que esteja no CCC efetivo, apenas com uma comunicação que se efetua hoje em dia com um telemóvel, através de uma imagem do controlo da situação a distância, com essa imagem consegue disponibilizar os recursos policiais que efetivamente sejam capazes de dominar a situação, para poder ter domínio da situação, a imagem do que se está a passar em tempo real é determinante”.

A simplicidade de utilização de um telemóvel com capacidade de transmissão de dados, abre uma janela de oportunidades sob o ponto de vista operacional, em forma de complemento a atividade no terreno, como referência Bruno Tomé “se a informação for mais assertiva, tem toda a lógica, em vez dos recursos estarem mais espalhados, eles poderiam estar com um foco mais assertivo”.

Outro aspeto, é com a qualidade da informação poder ser melhorada, atendendo a que como refere Bruno Tomé “por vezes a informação que é recolhida, é muito vaga, muito ampla, o que dificulta neste caso a alocação de recursos humanos”. “Se ela fosse mais assertiva, mais concisa, deste modo os recursos humanos poderiam ser canalizados de forma mais assertiva nas situações locais ao nível da prevenção”.

Um dispositivo seguro e simples de comunicação de dados, como refere Manuel Faustino pode reforçar o “agente policial que se encontra no terreno, efetivamente, o chamado polícia de giro, que são a grande massa das ações policiais, que fazem o trabalho de proximidade, o primeiro elemento de esquadra, piquete, posto que é disponibilizado para as situações e é o primeiro a chegar”, concomitantemente “havendo a disponibilidade no CCC em que nós tivéssemos a perceção clara do acontecimento do momento, seria possível encaminhar o agente sobre o que deve fazer, através do

telemóvel com a *checklist*. A *checklist* é importante, se nós catalogarmos às situações, isto acontece muito por exemplo com os Estados Unidos, os americanos fazem muito a catalogação para saber quando há um incidente, o que correu mal, para que não volte a acontecer”.

Um interface de telemóvel com uma App segura, como refere Manuel Faustino, conjugado com a “IA que temos hoje disponível, através dos meios informáticos, bastaria o agente clicar a tipologia do incidente e se tivermos uma *checklist*, além do controlo , é um auxílio, porque o agente a partir dai, perante o stress da situação, perante a ação, o ser humano tende a reagir de forma diferente a cada situação, posso ser um individuo calmo que reage com ponderação ou ser um outro individuo que não reage tão bem, que reage sobre brasas, o stress é normal, se tiver um alerta com ele e o possa dizer nesta situação, para ter atenção a determinadas situações, observar estes e estes pontos, as maiores falhas, uma *checklist* para diminuir o erro na obtenção de prova por exemplo, não é repetitivo, as situações não se repetem na vida. Para eliminar o erro no âmbito por exemplo da obtenção de prova, o agente estaria numa fase diferente pois estaria a obter um treino dentro do próprio trabalho”.

Uma outra vertente que se abre com um sistema de informações mais consistente, é poder-se consolidar, como expõe Luís Elias “o policiamento preditivo consiste em procurar antecipar o cometimento de perigos, atualmente temos ferramentas que podem fazer isso, o problema é que a crescente automatização, o *big data*, a correlação entre bases de dados, a georreferenciação, criam novas oportunidades, hoje já é possível analisar tendências de locais, como hotspots, ou sejam locais geográficos onde há uma grande concentração de crimes. O mais importante nisto tudo, é a capacidade de através do *big data* analisar tendências de longo prazo”.

A IA como vetor de auxilio nas varias vertentes da atividade policial como refere Luís Elias cria a “vantagem clara que a análise de dados criminais, pode trazer para a parte mais operacional da polícia, na perspetiva mais reativa, assim como na perspetiva da investigação criminal, onde poderá permitir a confrontação de suspeitos, em cenários de individuos que são detetados numa cidade, mas, estão a atuar em outra, a descrição das vítimas sobre as ocorrências, em termos de características, (forma de vestir, estatura, etc.), estas descrições do ponto de vista analítico podem ser muito importantes para no meio da panóplia de dados,–consigamos identificar esses suspeitos, noutras

ocorrências que sejam reportadas. Isto é muito útil, pois permite criar vantagens nas três vertentes, da prevenção criminal, da investigação criminal e da ordem pública”.

O aprimorar de informações tratadas são extremamente importantes no planeamento das operações de segurança, Pedro Clemente realça que “ Obviamente que sim, uma coisa é estar perante manifestações realizadas por entidades que já as fazem há muitos anos em que já são conhecidos os procedimentos, outra é quando estão organizações quase inorgânicas, ou seja, entidades com pouca estrutura em que não as conhecemos, e sobretudo hoje em dia é importante com os novos movimentos sociais que surgem por vezes com cariz violento, a preparação para evitar que isso aconteça é muito importante”.

O acesso a informação produz um planeamento operacional preditivo, no cenário relatado, Pedro Clemente enfatiza “muitas vezes as manifestações querem obter determinado tipo de resultados, ... por obrigar a polícia a fazer uma carga mais forte, se nós obtivermos a informação devida, poderemos usar meios mais adequados, de contenção pacífica, como barreiras e deste modo contrariar o jogo do adversário”, desenvolver a capacidade de tratar grandes volumes de dados, usando IA reforça o modo de auxílio preditivo.

As implementações destas soluções tecnológicas estão sujeitas aos limites da lei, como refere Manuel Faustino, embora, “as polícias normalmente estão a correr atrás do acontecimento, no entanto esta assimetria é um problema legal, normalmente o legislador vai atrás do acontecimento de forma reativa. A salvaguarda dos direitos, liberdades e garantias, imaginemos a situação em voga, as câmaras de vídeo vigilância, a utilização de *drones*, utilização das *bodycams* a exemplo, é inevitável, mas, temos uma limitação legal em termos de proteção de dados, da proteção de imagens e aqui temos um choque, que é a necessidade coletiva de proteção e a necessidade individual daquela pessoa em concreto. Esta parte da gestão do recurso e da formação virtual é por demais importante, pois, todos os meios tecnológicos ao dispor poderiam ser utilizados mais corretamente, para potenciar o homem”.

6.3. 3.^a PERGUNTA DERIVADA

A preparação do homem na aceitação da mudança e de forma a olhar o desenvolvimento tecnológico como uma ferramenta para o seu auxílio pessoal, da organização, do serviço judiciário e da sociedade em geral, aludindo a Manuel Anes,

“em primeiro lugar mudar a mentalidade do agente ou inspetor. É fundamental, pois se ele continua agarrado ao lápis e papel e a máquina de escrever reage contra a inovação, ora a inovação é fundamental, poupa tempo, procede a um melhor arquivo de toda a informação que estiver a ser recolhida e pode guiar os comportamentos profissionais do agente no terreno, de forma muito importante”.

Para que processos revolucionários com procedimentos novos, possam efetivamente ter sucesso é necessário, acautelar aspetos da natureza humana em matéria de capacitação e compreensão de causa-efeito da mudança, citando Manuel Faustino, “há toda a necessidade de dar à agente formação, de forma, a ser cada vez mais capaz. A necessidade da formação do homem é importante, a experiência passada no tempo do Windows 3.11 ainda em inglês nos anos 90, vivida por mim com alguns colegas mais idosos à época, em que na mudança da máquina de escrever para o computador, o que foi um grande avanço, agora imagine o avanço para alguém que deixou de substituir o papel quando se fazia um erro, pois um relatório com quatro ou cinco paginas, quando se estraga uma pagina por vezes era necessário fazer tudo de novo, quando o chefe corrigisse, frequentemente tínhamos que voltar a datilografar as correções”.

De igual modo, narra Manuel Faustino, “a evolução histórica para o computador, veio facilitar todo este processo”, pois proporcionou uma mais-valia na qualidade, rapidez de edição de documentos, possibilidade de produzir vários exemplares, traduzindo-se em economia de tempo na execução e acesso aos documentos informatizados.

No entanto, anos depois, quando surgiu a versão em Português do programa que então era utilizado no computador, descendeu a substituição da versão em inglês para a versão em português, esta comutação criou um processo inverso ao esperado, tendo desencadeado a repulsa pelos utilizadores ao uso do computador, atendendo a que o conhecimento até então adquirido deixou de valer, citando Manuel Faustino “de tal modo que alguns queriam voltar para a maquina de escrever, isto foi ultrapassado com as explicações que tivemos de dar aos colegas. Este pequeno exemplo, espelha bem o impacto da tecnologia e a necessidade de formação”.

Aparte a preparação do homem, utilizar um dispositivo tecnológico como um telemóvel ou um tablete seguro, na interatividade entre o agente no terreno e a sua retaguarda, de modo a assegurar o registo de ocorrências em tempo real, com reflexo na partilha do registo com o CCC possibilita o monitoramento a distancia e acompanhar o evoluir da ocorrência, como enfatiza Bruno Tomé, “possuir um meio tecnológico para logo de

imediatamente, quando estiver a tomar conta da situação de uma forma simples, só a nível de toques e enviar, torna-se tudo mais rápido, por outro lado quem recebe essa informação, consegue pegar em toda essa informação e limitar e dar informação *on-job*”, de modo ao agente no terreno poder ser auxiliado pelo processamento de IA ou por intervenção humana.

Para reforçar essa necessidade de ser auxiliado por uma ferramenta tecnológica, aludo a Bruno Tomé, “para se atingir esse nível é necessário a sensibilidade de quem anda no patrulhamento a preencher esses campos, pois muitas vezes quem anda na rua não tem tempo, por vezes tem de passar tudo a papel e de seguida enviar um e-mail para enviar um formulário”.

A utilização de IA, agregando o processamento de imagens digitais, Bruno Tomé menciona “no caso dos acidentes rodoviários, deveria existir já uma plataforma, que permitisse colocar logo tudo ao nível de quantos feridos, graves, ligeiros, automaticamente, carregar-se sem recorrer ao papel, ... isso ajudava bastante, para já facilitava ao nível do trabalho, e também permitia ter toda estatística, de quantos acidentes rodoviários ao nível nacional. A nível de crimes também é interessante, por exemplo, ter este tipo de tecnologia, acho que a tablete é ideal para o terreno, ajudava para já a tirar fotografias, preservava os indícios, e seria mais fácil, podiam gravar qualquer coisa ao nível de prova”.

A implementação desta interação, deve observar os limites legais como narra Luís Elias, “há um conjunto de garantias nos estados de direito democráticos que de alguma forma criam obstáculos à aplicação prática de algumas dessas tecnologias, tendo em conta os atuais quadros legais em vigor, os regulamentos europeus de proteção de dados, etc.”, de qualquer modo isto é um processo evolutivo.

A sociedade civil e o mercado tecnológico, como agentes sociais, por si só também são agentes da mudança, citando Luís Elias “as empresas tecnológicas continuam o seu desenvolvimento imparável, haverá um momento em que as tecnologias se alinharão a realidade, isso já acontece todos os dias, em vários âmbitos da nossa vida pelas ferramentas que vão sendo criadas e difundidas na vida prática, tais como *drones*, sistemas de vídeo e vigilância, a análise da *human intelligence*, há um conjunto de uma vasta panóplia de ferramentas que vão impondo a realidade”.

Ao nível da atividade operacional, para a recolha situacional, Bruno Tomé enaltece, “em cenários em que uma porta foi rebentada, está toda partida, eles poderiam tirar fotografias ou filmar a registar esse fato, possibilitaria a quem estivesse a reconstruir esse fato, era mais fácil entender como foi feito o assalto, ou porque assaltaram aquela casa? porque era mais fácil? estava isolada? não tinha medidas de segurança? Nestes aspetos, era fácil ao nível da tecnologia ajudá-los, e já saberiam que determinados tipos de casas eram visados pelo crime, possibilitaria um estudo e deste modo poder-se-ia canalizar os recursos para uma determinada zona de forma a impedir que isso voltasse a acontecer”.

Na observação do quadro legal, Luís Elias salienta, de igual modo as assimetrias entre os países na adoção de soluções, por limitação legal, “a ausência de regulação e controlo constitui um risco, pois a tecnologia avança mais rapidamente que a lei, portanto os estados com uma decisão política mais flexível, mais célere, que se adaptam mais rapidamente, podem contaminar os outros mais tradicionalistas. A nível da vídeo vigilância nos espaços públicos, havia muitos obstáculos a cerca de 20 anos, hoje já largamente aplicada nos países ocidentais e não ocidentais, em Portugal já temos muito mais locais a serem objeto de sistemas de vídeo vigilância em espaço público”.

A segurança é uma missão de todos os seus atores e Luís Elias evidencia que a “vigilância por parte do cidadão, este não pode abdicar dos seus direitos em prole de mais segurança, convinha que o equilíbrio necessário entre liberdade e segurança seja o mais balanceado possível, viver em sociedades assépticas e seguras, corre-se o risco de ver os direitos individuais serem devassados pelas diversas entidades”.

Salientando o aproveitamento da oportunidade criada pela tecnologia, de encurtar distâncias ao nível do empoderamento do homem, ao tornar uma ação complexa e limitada a equipa presente, poder transformá-la em um processo mais célere, apoiado e inspecionável, Manuel Anes reforça “a IA possibilita melhorar a rapidez de acesso a informação, temos de começar a trabalhar já no presente e futuro”.

6.4. A PERGUNTA CENTRAL

Quais os principais contributos da IA para o processamento de imagens a utilizar na segurança pública?

A predominância da opinião evidenciada nestas entrevistas é de que a AI tem papel fundamental e estratégico como auxiliar do profissional de segurança na geração de

informações operacionais relevantes para o auxílio à tomada de decisões e causar impacto no aumento crescente do desempenho da FSS, para o incremento da SP.

A importância da utilidade de IA é altamente relevante, citando Pedro Clemente, “hoje, a Polícia não passa sem Inteligência Artificial, tem de ser um modelo sistémico que integre as diversas plataformas e simultaneamente seja integrador, para que as bases de dados falem entre si, é preciso falarem, pensar em todos os sistemas de forma integrada, seja na observância da via pública, ou dentro de um estádio de futebol, até uma participação de um cidadão que fez uma denúncia anónima ou não, através de uma esquadra virtual”.

Na vertente de melhorar o desempenho do homem policial, Manuel Justino realça, “o principal contributo da IA na investigação é mitigar o erro, reduzir ao mínimo admissível o erro humano”, está observação enquadra-se na vertente da IA como auxiliar operacional dos efetivos no terreno, promovendo transparência, assertividade nos procedimentos operacionais, atendendo as circunstâncias de cada ocorrência.

Outro aspeto de ganho do desempenho é a possibilidade de monitoramento operacional dos efetivos no terreno, por parte, de quem tem a missão de coordenar e salvaguardar a integridade física de todos os envolvidos, bem como o sucesso da missão, sendo tarefa principal do CCC, a facilidade com que a informação pode fluir de um espaço para o outro em tempo real tornando-se uma alavanca poderosíssima de avaliação, intervenção e mitigação do erro humano.

Como resultado da utilização de IA, Manuel Anes enumera relevantes ganho diretos, “Identificação de suspeitos é fundamental, a georreferenciação das ocorrências”, o registo de imagens digitais enviadas pelo cidadão através da esquadra virtual, como conteúdo das denúncias, após validação, podem ser processadas por IA para identificar o local georreferenciado pela análise de metadados, reconhecer os suspeitos, descobrir correlações com os objetos implicados e, encontrar conexão com outros crimes registados.

Em termos tecnológicos, já existem disponíveis alguns produtos que realizam estas identificações como refere Luís Elias, “a tecnologia dá-nos grandes perspetivas de identificar suspeitos, potencia o combate ao crime organizado e violento, há sistemas de reconhecimento facial, deteção de padrões e outros, implementados em alguns países”, no entanto, o sucesso na obtenção de resultados favoráveis, depende

essencialmente da organização possuir de antemão grandes volumes de dados e acesso a *big data*, só assim se pode obter um horizonte de comparação admissível a integração de IA.

A utilização de IA já registou resultados favoráveis como expõe Luís Elias, “houve já muitos sucessos fruto dessa tecnologia, já foram evitados atentados porque os sistemas de vídeo vigilância, tinham acoplados *software* que detetam desvios ao padrão, o caso de um carro estacionado em local proibido em hora estranha, leva a que o centro de comando e controlo, desencadeie para lá meios para averiguar as razões do carro estar em local indevido, e neste caso em concreto as averiguações detetaram explosivos, isto aconteceu na cidade de Nova Iorque, na *times square*”, quando estão reunidos os pressupostos necessários ao alto desempenho de IA, o processamento de imagens digitais por IA pode contribuir de modo expressivo o incremento da SP.

Estes resultados são exequíveis, segundo Bruno Tomé, porque “a IA trata de forma mais rápida em comparação com a nossa visão, na segurança pública em zonas em que acontece algum crime, nós por algumas características desse sujeito, poderíamos encontrar mais facilmente o suspeito”, existem muitas possibilidades de critério de pesquisa, desde a análise de padrões, o reconhecimento facial, o *modus operandi*, etc. a conjugação dos diversos critérios de raciocínio, abrem caminho a uma revolução na clássica forma da análise de dados.

O policiamento preditivo ganha com a IA um auxiliar de grande monta, atendendo a sua capacidade, conforme Luís Elias, “a capacidade adicional que há de detetar situações suspeitas, que se podem confirmar ou não, também se aplica a indivíduos, outra utilidade grande está na deteção de bagagens abandonadas em aeroportos, estações de caminho de ferro ou outras, para alertar e desencadear o processo da ação humana, na verificação desses alertas que podem corresponder a um agente explosivo que ali foi plantado dolosamente”, a predição desencadeada pela análise de imagens digitais, possibilita operar por antecipação, resultando por vezes na confirmação de ameaças.

As utilidades praticas de IA são variadas, consoante Bruno Tomé, “vejo muitas vantagens na utilização de IA, o reconhecimento facial, a nível de imagens, e vai facilitar nos carros modernos, determinadas características que a IA vê, em aglomeração de pessoa junto a passadeira procede a redução automática da velocidade. Se tivermos isso implementado quando houver um afluxo grande de pessoas na passadeira e o semáforo passar gradualmente de verde para laranja e depois vermelho, vai fazer com

que a viatura que se aproxima em alta velocidade, comece logo a diminuir velocidade e por outro lado facilitar a passagem dos peões em segurança, isto seria uma ajuda na prevenção de acidentes rodoviários, de multas e outros”, este é um bom exemplo de prevenção rodoviária, com resultados no aperfeiçoamento da SP.

Outra utilidade adicional, por Bruno Tomé é “a IA pode ser um auxiliar para quem está no terreno, na atualidade por muito boa informação que se dê, os agentes por vezes estão envolvidos em tanta coisa ao nível legal, necessitam de saber de muitas leis e é muito difícil, a solução pode ser uma app, para tornar mais fácil e de forma simples, tratar a informação concisa, as pessoas não teriam de escrever muito, só teriam de selecionar, a recolha de dados para quem anda na rua, num formato de relatório de atualização periódica para acompanhar as mudanças da lei.

A sumula do progresso inovativo, alcançado pela sistematização operacional da recolha de dados, como refere Bruno Tomé vai “permitir registar os contributos dos agentes num campo de questões relevantes, para futuramente poder ser avaliada a relevância desse dado para atualizar o relatório, automaticamente teríamos informação mais concisa e iríamos melhorando no dia a dia”, este processo de recolha de dados promove a melhoria continua e, produzir aumento de desempenho nas FSS, seja na mitigação do erro humano, mas também em termos processuais no qual, ao tornar mais ágeis a produção de relatórios pela facilidade de registo das ocorrências, fomentando o agilizar do processo judicial, como um contributo direto a SP.

A segurança na dimensão da EU, caracteriza-se por aspetos circunscritos a cada estado e comuns aos estados da União, no qual o processamento de imagens digitais tenha na IA, um veiculo de reforçar o controlo da circulação de pessoas procuradas pela justiça, como refere Manuel Faustino, “no contexto europeu, por se terem suprimido as fronteiras internas e atendendo a que cada estado tem a sua própria politica de segurança interna, os protocolos e a colaboração entre estados não chegam para o controlo, é necessário colocar a tecnologia ao serviço da União Europeia, independentemente das policias que existam, quando estamos perante um criminoso no contexto europeu no qual os estados não são estanques em termos de circulação de pessoas e bens, mas, são estanques em termos de aplicação de justiça”.

No princípio da realização integrativa das varias Nações Europeias em matéria de segurança, Manuel Faustino destaca que um dos requisitos determinantes para o bom andamento dos projetos comuns, é a barreira cultural entre os povos, na perceção da

realidade de cada um, que por motivos óbvios, acentuam o juízo de valor de uns pelos outros, mesmo falando a mesma língua, destacam-se obstáculos de linguagem, “ Os principais contributos na utilização dos meios tecnológicos, rapidez, separação, formação, capacidade de comando e controle, no espectro nacional entre as várias forças e UE entre os vários Países e as suas forças, o determinante é definir uma linguagem comum. A tecnologia é extremamente importante, a IA será certamente importante, mas, as premissas de ação, de alertas e tudo o mais, têm de ser comuns, ser perceptíveis, ser entendíveis, temos de falar a mesma linguagem, para potenciar o entendimento entre todos”.

Já Paulo Nicolau menciona que “no âmbito da segurança pública, considero que um dos eventuais contributos poderá ser ao nível do reconhecimento facial, depois de devidamente dirimidas as questões inerentes à salvaguarda dos direitos, liberdades e garantias dos cidadãos”.

Agora Manuel Faustino alude que “o acesso em tempo real para verificar dados, traduz-se na diminuição do tempo de aplicação da justiça, ao diminuir o erro, estamos a dar a capacidade de o investigador fazer a sua análise, correlação e síntese, maximização da capacidade e a justiça na aplicação do direito. O legislador ao criar restrições está no pressuposto da preservação da pessoa humana, na legalidade dos factos, na defesa dos visados, mas na verdade pode estar a fazer o contrário, porque se se aplicar a justiça fora do tempo, já se estiverem legalizados os meios tecnológicos poderemos de uma forma normal ter uma justiça mais célere.

Pretendo destacar a agilidade alcançável na produção de processos judiciais, com premissas mais esclarecedores, atendendo a capacidade de registo minucioso das ocorrências, complementado pela IA ao extrapolar informações, dos dados históricos, produzindo um auxílio adicional na investigação, com a validação de conformidade da recolha registada e, na facilidade de produzir o processo judicial, como destaca Manuel Faustino, “ Isto é muito importante, para se fazer justiça, quando não se utilizam os meios tecnológicos por força das restrições, normalmente, teremos mais dificuldades em fazer justiça”.

O respaldo da lei para o progresso é outro aspeto importante que Manuel Faustino referencia “Quando se fala em aplicar tecnologia às forças de segurança, temos pelo menos dois impedimentos, sendo o primeiro o aspeto legal, o segundo a carga da doutrina interna, por outro lado, na aplicação da IA um desafio importante a considerar

é o impacto do aumento ou diminuição do poder em alguns atores da segurança, com reflexos na resistência a mudança.

Um das grandes condicionantes para o êxito de soluções tecnológicas é o alinhamento do homem com a necessidade de saber utilizar os interfaces aplicativos, atendendo a que em termos geracionais, estas soluções tecnológicas são muito novas, há a necessidade de desenhá-las de forma inclusiva, sem deixar ninguém de fora, conforme refere Pedro Clemente, “é preciso incorporar principalmente os mais velhos, nestas novas tecnologias, para explorar esta nova informação”, embora o esperado seja a simplificação de processos, por vezes, o que é simples para uma geração que se desenvolveu na era da sociedade da informação, pode ser uma complicação para as gerações anteriores, desta maneira, estas iniciativas devem ser planeadas contemplando as sensibilidades de todos os elementos das FSS, pois só assim se estabelecem bases para o combate de resistência a mudança, enquanto elemento crucial para o êxito de projetos tecnológicos.

A utilização da máquina como auxiliar, é somente um complemento da capacidade humana, no final quem prepara os algoritmos são os humanos, a sensação de desconfiança da máquina, fruto da ficção científica vulgarizada pela indústria cinematográfica, no qual os computadores poderão obter o domínio da vontade humana, não devera constituir uma preocupação para as gerações futuras, simplesmente porque a tecnologia com está concebida, necessita de energia elétrica para operar e, nós os humanos estaremos sempre em posição de poder desligar as máquinas.

A força da inteligência humana é tao preponderante, não se deve descurar que a IA é somente mais um auxiliar, a todas as espécies clássicas de obtenção de informações, como reforça Luís Elias “um aspeto que não nos podemos esquecer, a tecnologia por si não pode ser aplicada em detrimento da *human intelligence*, que esta tecnologia não faça a polícia abandonar o contato com as comunidades, com os informadores, senão corremos o risco de ter somente uma perspectiva assética da realidade”.

Luís Elias reforça ao referir “é importante que esta evolução tecnológica seja acompanhada na continuidade da aposta com trabalho no terreno, que até ver são os humanos a fazer, mesmo antevendo um enorme desenvolvimento tecnológico, não devemos abandonar a *human intelligence*”, o homem primeiro, como uma frente humana de características únicas, desde a inteligência emocional, a ética do bem comum, o livre arbítrio e, a liberdade conquistada em democracia,

A ciência tecnologia sempre que racionalmente aplicada, promove desenvolvimento social, económico, político, ambiental, segundo Manuel Anes “a ciência é uma coisa boa, ... a ciência é muito importante, venha ela com os auxílios como a IA, que é um grande auxílio, um grande contributo para segurança de todos nós”.

7. CONCLUSÕES E RECOMENDAÇÕES

Pelo conhecimento recolhido com as entrevistas, suportado pelos conceitos identificados, que gravitam a volta do tema, relacionado pelo momento tecnológico que vivemos em matéria da capacidade de computação e a evolução alcançada pelas infraestruturas de comunicações, estaremos perante um momento singular do alinhamento de tecnologia, conhecimento e necessidade de maior celeridade operacional.

7.1. CONCLUSÕES

A predominância da opinião evidenciada nesta pesquisa, é de que, a AI tem papel fundamental, como coadjuvante do profissional de SP, na geração de informações nos diversos seus níveis, estratégico, operacional e tático, de maneiras pertinentes para o auxílio à tomada de decisões que influenciam a assertividade da securitização social, gerando o aumento da sensação de segurança.

A quantidade de obras analisadas nesta pesquisa revela uma limitação metodológica a ser considerada, devido às publicações sobre este tema ainda serem poucas, entretanto este trabalho tem a sua relevância, mesmo com restrições na disponibilidade do acervo académico, por buscar discutir e compreender o papel da inovadora tecnologia de AI nos sistemas de gestão da Segurança Pública, aguçando as sinergias entre esse fenómeno tecnológico e o profissional de Segurança Pública moderno.

Esta pesquisa identificou a sinalização de sete elementos quão úteis para a inovação das FSS, o homem, a tecnologia repartida em dispositivos táticos como telefone, tablete, ao nível do software, as Apps de recolha de dados, a centralização das bases de dados, a esquadra virtual e acompanhamento das ocorrências em tempo real, conjugado com processamento de imagens digitais por IA, de forma a reforçar a vigilância inteligente.

Ficou sinalizado como 1º elemento, que sem a componente humana devidamente preparada, o êxito de utilização de tecnologia no auxílio do profissional das FSS, pode redundar em fracasso, em primeiro plano por rejeição a mudança, embora no fundo possa ser essencialmente falta de conhecimento, por este não ter recebido a formação necessária, com a devida interiorização de causa-efeito, o que possibilitara o alinhamento do homem com a solução tecnológica.

Esta pesquisa aponta que o uso da IA traz muitas avanços para os profissionais de segurança, seja reduzindo o tempo que estes despendem em trabalhos rotineiros, repetitivos, passando a gerar informações preciosas de forma estruturada e, oportunas em menor tempo para que, sobre mais tempo, maior racionalização dos recursos disponíveis, para atividades com mais diferencial operacional e tático potenciando a produtividade.

A sinalização do 2º elemento, sendo os dispositivos tecnológicos disponíveis, o qual apontam o telefone e, a tablete, como ferramentas de apoio tático aos profissionais de segurança, atendendo a que, são de fácil portabilidade, com elevado grau de uso social, por ser uma ferramenta já largamente utilizada para outros fins, em suma, podemos considerar que são um utensílio generalizado na vida das pessoas.

O telefone e a tablete para este fim só diferem em tamanho, no entanto é importante salientar que é mais fácil transportar e operar no telefone por caber no bolso, o ponto contra é o tamanho do ecrã, mas, o processo social e tecnológico de inovação da recolha de dados, caminha para um sistema de recolha de dados pré-registados, a exemplo em dado sinistro rodoviário, para identificar os veículos bastara apontar a camara do telefone para a matrícula, esta imagem digital produzida, em automático desencadeia um processo de IA, que preencherá o formulário de forma automatizada.

A recolha de imagens digitais, facilita o preenchimento da ocorrência, com os dados do veiculo, dados do seguro, dados do proprietário, a carta de condução bastara digitar o numero, no entanto tão logo se percebe, ao nível administrativo a necessidade dos documentos possuírem elementos óticos de identificação como o *QR code*, estes ficarão mais facilitados, outro meio de preencher os dados dos envolvidos, é a utilização da câmara do telefone, na recolha de imagem digital, como auxiliar de IA no reconhecimento facial.

Outra facilidade com o telefone é ser igualmente utilizado para registar os testemunhos dos envolvidos, com vídeo e som, ou somente som, de igual modo, obter registo de vídeo de objetos, relevantes para a ocorrência.

Ao nível do software, o 3º elemento assinalado destaco as Apps, que na realidade são programas de iteração entre o homem e o dispositivo tecnológico, é com a utilização das Apps que habilitamos a capacidade de troca de dados, seja de recolha, validação, retorno de informação, é com a utilização das Apps que se passa para o sistema de

entrada única de dados, diminuirá ou deixará de ser necessário os profissionais de segurança sentarem-se ao computador para preencher formulários ou relatórios, pois os dados já terão sido previamente digitalizados, trata-se de um salto de inovação e mudança, enquadrada na transformação digital, como uma consequência direta do desenvolvimento tecnológico.

O 4º elemento assinalado, centralização das bases de dados, este elemento abrange os dados dentro de cada organização e de igual modo para o total das FSS, começando por Portugal, mas também, sem descurar a necessidade de alinhar o espaço de cooperação policial e judicial europeu, é manifestamente crucial a centralização dos dados, de forma que os interlocutores falem a uma só linguagem, pois permitira operar apoiada num horizonte visual bem mais acutilante.

A Esquadra virtual é o 5º elemento, por poder possibilitar ao cidadão apresentar participação por queixa de forma eletrónica, com identificação ou anónima, queixas criminais, público, privada e semipúblico, este serviço deve ser visto como uma inovação ao serviço 112, no qual o participante acedendo a esquadra virtual, poderá preencher os dados da queixa, anexar imagens, áudio, interagir com o *chatbot* para esclarecimento, escalar para o operador do serviço 112 se necessário, deste modo passarão a estar reunidas as condições de recolha de mais uma frente de dados em quarentena, que após validação, poderão ser considerados no expediente diário.

Este tipo de solução, é mais uma via de obtenção de imagens digitais facultadas pelo cidadão, no exercício da cidadania, a análise do material das queixas será alvo de escrutínio, com capacidade de ser divididos e agrupados por cada serviço de especialidade, sem substancial intervenção humana.

O empoderamento do Centro de Comando e Controlo é 6º elemento, a conjugação do homem, do telefone, da App, associada a capacidade de transmitir em tempo real, os dados de resposta a uma ocorrência, transforma o CCC na sua capacidade de intervir com maior incisão nos casos mais complexos e contribuir com a colaboração devida, de acordo com as circunstâncias.

Obter dados em tempo real, principalmente nos centros urbanos, onde a comunicação o permita, irá desencadear novos processos de interação entre o CCC e o PS, o recebimento de dados da recolha efetuada de hora de chegada, tipificada a ocorrência, número de elementos envolvidos, registo de imagens, arquivo de som dos testemunhos,

relatório verbal da situação pelo profissional de segurança e, muitos outros, estarão criadas condições para uma nova maneira estruturada de colaboração com as equipas no terreno.

A utilização de Inteligência Artificial é o 7º elemento assinalado, capacita os computadores nas mais variadas formas, servidores, computadores de mesa, tablete, telemóveis, câmaras fotográficas digitais, relógios *smart*, automóveis, etc., no sentido de poderem ver e ouvir com precisão varias vezes superior aos humanos, é esta capacidade, que pretendo dissertar através da pesquisa realizada, permitindo aproximar o homem da maquina, no apoio a decisão, atendendo a fatores em que a maquina supera o homem, tais como, capacidade de memoria, o computador não se esquece do que sabe, a velocidade de processamento, o computador processa grandes e complexos volumes de dados num piscar de olhos.

A IA congrega a facilidade e a agilidade em extrair e agregar metadados de imagens digitais, sobre homens, mulheres, crianças, veículos, objetos, tamanho, cor, velocidade, caminho, antecedentes e, muito mais, em formatos quantitativos, qualitativos, de abeiramento, de separação isolada, comparativa, abrindo novos horizontes de investigação criminal, na ordem pública, como auxílio a decisão estratégica dos profissionais de segurança pública.

Na Segurança Pública, a IA como ferramenta utilitarista, pode ser utilizada para prever e identificar os padrões do policiamento preditivo, tendo como ponto de partida os metadados relativos a violência e ao crime, no entanto existe o risco de a automação ficar dependente de despachos administrativos, como mera ferramenta de auxílio, por ter de carecer de autorização administrativa a sugestão gerada pela IA para a sua implementação.

A segurança pública mescla a definição clara dos eventos de interesse, a contagem dos eventos e a posterior análise desses eventos respeitante a pessoas, objetos, locais e hora, ao delegar tarefas de revisão de análise de dados com IA, passaremos a compreender mais rapidamente, incidentes e tendências de segurança por georreferenciação,

Este elemento IA, associado ao algoritmo de aprendizagem, são determinantes com a integração do homem, as Apps, a centralização dos dados, a esquadra virtual e acompanhamento das ocorrências em tempo real, conjugado com processamento de

imagens digitais por IA, as associações destes sete elementos resultam no processo de inovação de auxílio a decisão e gestão dos profissionais de segurança na manutenção da Segurança Pública. Produzindo o acelerar da capacidade de investigação, especialmente sempre que envolva ver e rever em grandes volumes de dados, para encontrar uma pessoa, um objeto e, deste modo gerar uma salva enorme de tempo, alcançando facilidade e agilidade.

Tentando antever, o produto direto desta mudança no auxílio a decisão dos profissionais de segurança com os elementos ora sinalizados, porém, integrados a realidade do desenvolvimento tecnológico, destaco o surgimento do 5G, o *IoT*, o *big data*, a mobilidade digital, posicionando-nos no momento histórico de viragem incomensurável, o resultado a esperar deverá ser um bem maior que o aqui expresso, pois tão logo se atinja este horizonte, por certo a perspicácia humana, estenderá este mesmo horizonte, para níveis que a imaginação no momento não me permite.

A tendência generalizada do uso das TI é uma inevitabilidade social e tecnológica, que já é indissociável do estilo de vida moderno, deste modo, a utilização de IA no processamento de imagens digitais pelos FSS é já uma realidade em diversos países, desde o Reino Unido, a China, a Austrália, o Canada, a França e muitos outros, no entanto em Portugal, tornar-se-á do mesmo modo inevitável, o alargamento da recolha vital de informação, atendendo a crescente simbiose da biologia humana com as máquinas de processamento eletrónico, potenciando a capacidade cognitiva dos utilizadores, será efetivamente somente uma questão de tempo até que se encontrem mecanismos legais para permitir de forma confidencial a recolha e armazenamento de dados, para posterior catalogação e poder ser utilizado como mecanismos de aumento da eficiência das FSS.

Graças às tecnologias de mobilidade digital, conjugadas com os processamentos de imagens digitais, podem contribuir para a realização dos objetivos de prevenção criminal, ou seja, reduzir o número de ilícitos criminais, evitar a prática sistemática de crimes e, assim, contribuir para a luta no aumento da segurança. As imagens processadas por IA podem fornecer informações aos operacionais presentes no terreno e, portanto, contribuir para incrementar na SP uma política mais proativa e menos reativa.

Como a tecnologia evolui a cada dia, sugere-se que futuros estudos sobre o tema sejam feitos a fim de se considerar uma amostra maior de trabalhos e a própria evolução tecnológica da Inteligência Artificial.

Concluiu pelas entrevistas, concordância na importância de se agregar mais valor a importante tarefa de assegurar a SP, através do desenvolvimento para a gestão do conhecimento objetivo, afim do empoderamento das várias camadas de intervenção das FSS, ser percecionada com uma vantagem objetiva, na vertente de mitigação do crime.

7.2. LIMITAÇÕES

Atendendo ao tema subjacente de segurança pública, constitui uma limitação natural, na relação com o secretismo envolvente, despertando a atenção especial na abordagem, constituindo-se uma barreira limitativa de aprofundamento de causa e efeito, sobre o estado atual dos sistemas existentes e a forma futura num cenário de IA.

Na realização deste trabalho, evidenciaram-se algumas limitações, constituindo-se como exemplos o tempo limitado dos entrevistados, assim como, conseguir alargar o leque de entrevistados, para se alcançar a recolha do conhecimento entre os vários atores com relevância na SP, estabelecendo um limite no número de sensibilidades registadas.

As restrições de circulação impostas pela pandemia de Covid-19, foram uma limitação material, no acesso a Literatura, desde o acesso físico a bibliotecas, delimitando a identificação e obtenção de publicações em temas relacionados.

7.3. PROPOSTAS PARA INVESTIGAÇÕES FUTURAS

Analisando o potencial do tema, impõe-se propostas para investigações futuras, este trabalho versou sobre o contributo que as imagens digitais, uma vez processadas por IA, podem ser um fator de empoderamento da atividade das FSS, numa perspetiva de integração mais profunda das novas tecnologias, tais como:

Avaliar a experiência obtida com os sistemas existentes de tratamento de imagens, na vertente das horas de trabalho e recursos policiais envolvidos, bem como, os resultados já alcançados.

Quantificar os resultados vivenciados com os meios tecnológicos em uso nas FSS, numa perspetiva do antes e do agora, para possibilitar no futuro próximo estatística comparativa real de custo, benefício.

Outra proposta, que se recomenda ser estudada, consiste em obter-se métricas da dificuldade, facilidade arroladas ao longo dos tempos em matéria de mudança, atendendo a fatores naturais de resistência a mudança, assim como, o efeito facilitador da aplicação tecnológica nos projetos de sucesso, em que se traduzam numa melhoria organizacional.

REFERÊNCIAS

ACKERMAN, Spencer (2013) - Welcome to the age of big drone data. Wired [Em linha]. (25 Apr. 2013). [Consult. 14 mai. 2022]. Disponível em WWW:<URL:https://www.wired.com/2013/04/drone-sensors-big-data/>>.

AL-KHALILI, Jim (2018) - What the Future Looks Like: Scientists Predict the Next Great Discoveries—and Reveal How Today’s Breakthroughs Are Already Shaping Our World. [S.l.] : The Experiment.

ALLEN, Gregory C. (2019) – Understanding China’s AI strategy : clues to chinese strategic thinking on artificial intelligence and national security [Em linha]. Washington : CNAS.ORG. [Consult. 14 mai. 2022]. Disponível em WWW:<URL:https://s3.amazonaws.com/files.cnas.org/documents/CNAS-Understanding-Chinas-AI-Strategy-Gregory-C.-Allen-FINAL-2.15.19.pdf?mtime=20190215104041>>.

ANDRADE, Manuel, (2006) - Sobre as Proibições de Prova em Processo Penal. Reimpressão. Coimbra : Coimbra Editora.

ANDREJEVIC, Mark (2016) - Theorizing drones and droning theory. In ZAVRŠNIK, Aleš, ed. - Drones and Unmanned Aerial Systems. New York : Springer. p. 21-43.

BERNARDI, Mariana Rocha (2019) - O uso indiscriminado da inteligência artificial : uma discussão ética [Em linha]. Caxias do Sul : Universidade de Caxias do Sul. [Consult. 14 mai. 2022]. Disponível em WWW:<URL:https://repositorio.ucs.br/xmlui/handle/11338/4856>>.

BOUCHRIKA, Imed ; NIXON, Mark S. (2006) - People detection and recognition using gait for automated visual surveillance. In IET Conference on Crime and Security [Em linha]. London : IET. p. 576-581. [Consult. 14 mai. 2022]. Disponível em WWW:<URL:https://www.researchgate.net/publication/224062435_People_Detection_and_Recognition_using_Gait_for_Automated_Visual_Surveillance>>.

CAMPOS DO JORDÃO (2013) - Plano Municipal de Segurança Pública Campos do Jordão – SP [Em linha]. Campos do Jordão : Município Campos do Jordão. [Consult. 18 mar. 2022]. Disponível em WWW:<URL:

http://camposdojordao.sp.gov.br/Arquivos_Publicacoes/PPA_LDO/23012020-031440-plano-municipal-seguranua-publica.pdf>.

CANOTILHO, Gomes ; MOREIRA, Vital, (2006) - Constituição da República Portuguesa Anotada : Artigos 1.º a 107.º. 4.ª ed. revista. Coimbra : Coimbra Editora. Vol. 1.

CAPUTO, Anthony (2014) - Digital Video Surveillance and Security. 2.ª ed. Amsterdam : Elsevier.

CASTELLIS, Manuel (2018) - O Poder da identidade. São Paulo : Edição Paz e Terra.

CHEN, Hsinchun ; WANG, Fei Yue (2005) – Artificial Intelligence for Homeland Security. IEEE Intelligent Systems [Em linha].20:5 (sep. 2005) 12-16. [Consult. 25 fev. 2022]. Disponível em WWW:<URL:10.1109/MIS.2005.88>.

CHEN, Hsinchun ; XU, Jennifer (2006) – Intelligence and Security Informatics. Annual Review of Information Science and Technology [Em linha]. 40 (2006) 229-289. [Consult. 25 fev. 2022]. Disponível em WWW:<URL:https://doi.org/10.1002/aris.1440400113>.

CHIAVENATO, Idalberto (1999) - Gestão de Pessoas. Rio de Janeiro : Edição Campus.

CLARKE, Arthur (1996) - 3001 The Final Odissey. New York : Random House Publishing Group.

COSTA, Catarina Rodrigues Santos (2017) - As proibições da prova e a prova digital : aproximação aos lugares-comuns de um instituto clássico em face de uma nova realidade [Em linha]. [S.l.] : Universidade do Minho. Dissertação de mestrado em Direito Judiciário (Direitos Processuais e Organização Judiciária). [Consult. 14 jan. 2022]. Disponível em WWW:<URL:https://hdl.handle.net/1822/51857>.

CRESSWELL, Tim (2014). Mobilities III : moving on. Progress in Human Geography [Em linha]. 38:5 (2014). [Consult. 14 jan. 2022]. Disponível em WWW:<URL:https://doi.org/10.1177/0309132514530316>.

DEFENCEWEB (2021) - Argos II HD to support Frontex maritime surveillance project. DefenceWeb [Em linha]. (24 Aug. 2021). [Consult. 14 jan. 2022]. Disponível em WWW:<URL:https://www.defenceweb.co.za/security/border-security/argos-ii-hd-to-support-frontex-maritime-surveillance-project/>.

DELOITTE ; CONFEDERATION OF INDIAN INDUSTRY (2018) – 5G : the catalyst to digital revolution in India [em linha]. Gurgaon : Deloitte. [Consult. 14 mar. 2022]. Disponível em WWW:<URL:https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-the-catalyst-report-one-noexp.pdf>.

DEMIREL, Özlem (2021a) - Priority question for written answer P-002276/2021 to the Commission : Rule 138. European Parliament [Em linha]. [S.l.] : European Parliament. Long-range drones for Frontex, European Parliament, 29 april 2021. [Consult. 18 jan. 2022]. Disponível em WWW:<URL:https://www.europarl.europa.eu/doceo/document/P-9-2021-002276_EN.html>.

DEMIREL, Özlem (2021b) - Question for written answer E-002455/2021 to the Commission : Rule 138. European Parliament [Em linha]. [S.l.] : European Parliament. Surveillance sensor technology of Frontex drones in the Central Mediterranean, 18 may 2021. [Consult. 18 jan. 2022]. Disponível em WWW:<URL:https://www.europarl.europa.eu/doceo/document/E-9-2021-002455_EN.html>.

DIAS, Jorge de Figueiredo (1974) - Direito Processual Penal. Coimbra : Coimbra Editora. Vo. 1.

DOMINGOS, Pedro (2017) – A Revolução do Algoritmo Mestre. Lisboa : Manuscrito.

ELIAS, Luís Manuel André (2011) – Segurança na contemporaneidade, internacionalização e comunitarização [Em linha]. Lisboa : FCSH. Tese de Doutoramento em Ciência Política. [Consult. 18 jan. 2022]. Disponível em WWW:<URL:http://hdl.handle.net/10362/14011>.

EUROPEAN UNION. Commission (2018) - A strengthened and fully equipped European Border and Coast Guard. State of the Union [Em linha]. (12 September 2018). [Consult. 18 jan. 2022]. Disponível em WWW:<URL:https://euagenda.eu/upload/publications/untitled-183061-ea.pdf>

EUROPEAN UNION. Parliament ; EUROPEAN UNION. Council (2019) - Regulation (EU) 2019/... of the European Parliament and of the Council of ... on the European Border and Coast Guard and repealing Regulations (EU) No 1052/2013 and (EU) 2016/1624 [Em linha]. Brussels : European Union. PE-CONS 33/19. FRONT 176; SIRIS

89; COMIX 252; CODEC 375. [Consult. 14 mar. 2022]. Disponível em WWW:<URL:https://data.consilium.europa.eu/doc/document/PE-33-2019-INIT/en/pdf2>.

FRANK, Malcom ; ROEHRIG, Paul ; PRING, Ben (2017) – What to do when machines do Everything. [S.l.] : Wiley.

FREIXO, M. J. V. (2009) - Metodologia científica : Fundamentos métodos e técnicas. Lisboa : Instituto PIAGET.

FRIEDERSDORF, C. (2014) - Eyes over Compton : how police spied on a whole city. The Atlantic [Em linha]. (21 April 2014). [Consult. 14 nov. 2021]. Disponível em WWW:<URL:http://www.theatlantic.com/national/archive/2014/04/sheriffs-deputy-compares-drone-surveillance-of-compton-to-big-brother/360954/>.

GONZALES, Rafael ; WOODS, Richard (2010) - Processamento Digital de Imagens. 3.^a ed. São Paulo : Pearson.

GREENWALD, Glenn (2014) – No Place to Hide. London : Penguin.

GRIJPINK, Ferry [et al.] (2020) - Connected world : An evolution in connectivity beyond the 5G revolution [Em linha]. [S.l.] : McKinsey Global Institute. [Consult. 18 mar. 2022]. Disponível em WWW:<URL:https://www.mckinsey.com/~media/mckinsey/industries/technology%20media%20and%20telecommunications/telecommunications/our%20insights/connected%20world%20an%20evolution%20in%20connectivity%20beyond%20the%205g%20revolution/mgi_connected-world_discussion-paper_february-2020.pdf>.

GUIMARÃES. Tribunal da Relação (2014) - Acórdão do Tribunal da Relação de Guimarães de 29/04/2014, processo n.º 102/09.8GEBRG.G2. Acórdãos TRG [Em linha]. Relator Maria Luísa Arantes. [Consult. 21 out. 2021]. Disponível em WWW:<URL:http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/de1d4cb28038581a80257cdf00465dff?OpenDocument>.

introduction by John G. Slater. London : Routledge.

IVOLELA NETO, Romeu (2019) - O Robô autodidata : representação mental e autonomia cognitiva em inteligência artificial [Em linha]. Porto FLUP. Dissertação realizada no âmbito do Mestrado em Filosofia – ramo de Filosofia. [Consult. 18 mar.

2022]. Disponível em
WWW:<URL:https://sigarra.up.pt/flup/pt/pub_geral.pub_view?pi_pub_base_id=363067
>.

JACKSON, Susan, ed. ; HITT, Michael, ed. ; DENISI, Angelo, ed. (2003) - Managing knowledge for sustained competitive advantage. [S.l.] : Pfeiffer.

JESUS, Francisco (2015) - Os meios de obtenção de prova em processo penal. 2.^a ed., revista, atualizada e ampliada. Coimbra : Almedina.

KARAMPELAS, Panagiotis ; BOURLAI, Thirimachos (2018) - Surveillance in Action. New York : Springer.

KARAMPELAS, Panagiotis, ed. ; BOURLAI, Thirimachos, ed. (2018)-- Surveillance in action technologies for civilian, military and cyber surveillance. New York : Springer.

KATZIS Konstantinos ; AHMADI, Hamed (2016) - Challenges Implementing Internet of Things (IoT) Using Cognitive Radio Capabilities in 5G Mobile Networks. In MAVROMOUSTAKIS, C., ed. ; MASTORAKIS, G.,ed. ; BATALLA, J., ed. - Internet of Things (IoT) in 5G Mobile Technologies. Modeling and Optimization in Science and Technologies. [S.l.] : Springer. Vol. 8.

KAUFMANN, Vincent ; BERGMAN, Manfred Max ; JOYE, Dominique (2004) – Motility : mobility as capital. International Journal of Urban and Regional Research [Em linha]. 28:4 (December 2004). [Consult. 18 nov. 2021]. Disponível em WWW:<URL: https://doi.org/10.1111/j.0309-1317.2004.00549.x>.

KLAUSER, Francisco (2004) – A comparison of the impact of protective and preservative Video Surveillance on Urban Territoriality : : the Case of Switzerland. Surveillance & Society [Em linha]. 2:2-3 (2004). [Consult. 25 out. 2021]. Disponível em WWW:<URL: https://doi.org/10.24908/ss.v2i2/3.3371>.

LAKATOS, Eva ; MARCONI, Marina (1992) – Metodologia do Trabalho Científico. Rio de Janeiro : Edição Atlas.

LEE, Kai-Fu (2018) – As Superpotências da Inteligência Artificial. Lisboa : Relógio D'Água.

LEMES, Marcelle (2019) – Inteligencia artificial, algoritmos e policiamento preditivo no poder publico federal brasileiro [Em linha]. Brasília : Universidade de Brasília, Faculdade de Direito. [Consult. 25 out. 2021]. Disponível em WWW:<URL:https://bdm.unb.br/bitstream/10483/24565/1/2019_MarcelleMartinsLemes_tcc.pdf>.

LIMER, Eric (2013) - Watch the world's highest resolution drone-mounted camera in action. Gizmodo [Em linha]. (27 jan. 2013). [Consult. 25 out. 2021]. Disponível em WWW:<URL:<http://gizmodo.com/5979372/watch-the-worlds-highest-resolution-drone-mounted-camera-in-action>>.

LIU, Xiaozi ; SHEN, Chao ; CHEN, Yufei (2018) - Multi-source interactive behavior analysis for continuous user authentication on smartphones. In ZHOU, Jie, ed. [et al.] - Biometric Recognition : 13th Chinese Conference, CCBR 2018 Urumqi, China, August 11-12, 2018, proceedings. Cham, Switzerland : Springer. p. 669-677.

MARIN, Luisa ; KRAJČÍKOVÁ, Kamila (2016) - Deploying Drones in Policing Southern European Borders: Constraints and Challenges for Data Protection and Human Rights. In ZAVRŠNIK, Aleš, ed. - Drones and Unmanned Aerial Systems. New York : Springer. p. 101-127.

MARQUES, Pedro Penha Leitão da Costa (2013) - Informática Forense : Recolha e preservação da Prova Digital. Porto : Universidade Católica Portuguesa. Dissertação para obtenção do grau de Mestre em Segurança em Sistemas de Informação. [Consult. 18 mar. 2022]. Disponível em WWW:<URL:<https://repositorio.ucp.pt/bitstream/10400.14/13191/1/Disserta%C3%A7%C3%A3o%20-%20Recolha%20e%20preserva%C3%A7%C3%A3o%20da%20prova%20digital.pdf>>.

MARQUESONE, Rosangela (2017) - Big Data : técnicas e tecnologias para extração de valor dos dados. [S.l.] : Casa do Código.

MATOS, Patrícia, (2018) – Nomadas digitais e a era dos sujeitos móveis : questões de mobilidade comunicação e trabalho num estilo de vida location independente. In ARAÚJO, Emília, ed. [et al.] - Viver em/a mobilidade : rumo a novas culturas de tempo, espaço e distância : Livro de atas [Em linha]. 36-48. Braga: CECS. [Consult. 18 mar. 2022]. Disponível em

WWW:<URL:http://www.lasics.uminho.pt/ojs/index.php/cecs_ebooks/article/view/2878>.

MAVROMOUSTAKIS, C., ed. ; MASTORAKIS, G.,ed. ; BATALLA, J., ed. (2016) - Internet of Things (IoT) in 5G Mobile Technologies. Modeling and Optimization in Science and Technologies. [S.I.] : Springer. Vol. 8.

MCCUE, C. (2006) - Data mining and predictive analysis: Intelligence gathering and crime analysis. Oxford : Butterworth-Heinemann.

MCINERNEY, Claire ; DAY, Ronald (2007) - Rethinking Knowledge Management. New York : Springer.

MEALY, Paul (2018) – Virtual & augmented reality for dummies. New York : Wiley.

MOREIRA, Ana Cláudia (2019) - Benefícios da Tecnologia no judiciário. Brasília : Universidade de Brasília.

MOTTA, Renata (2009) - Simpósio proporciona debates intensos com convidados nacionais e internacionais. In BEIGUEIMAN, Giselle [et al.] – Apropriações do (in) comum, espaço público e privado em tempos de mobilidade [Em linha]. São Paulo : Instituto Sérgio Motta. [Consult. 18 mar. 2022]. Disponível em WWW:<URL:http://www.hrenatoh.net/curso/textos/_artemov_port_.pdf>.

Moura, Debise, (2018) – Mobilidade: O percurso do conceito e sua aproximação a comunicação - Livro de Atas - Viver em Mobilidade rumo a novas culturas de tempo e espaço e distancia, 28.

NEVES, Rosa Vieira (2011) - A Livre Apreciação da Prova e a Obrigação de Fundamentação da Convicção. Coimbra : Coimbra Editora.

O'BRIEN, Stuart (2020) – Number of cctv cameras in the UK reaches 5.2 million. Security Briefing [Em linha]. (20 Nov. 2020). [Consult. 18 mar. 2022]. Disponível em WWW:<URL:<https://totalsecuritysummit.co.uk/briefing/number-of-cctv-cameras-in-the-uk-reaches-5-2-million/>>.

OLIVA, Diego Coletti (2015) - Em busca da segurança : tecnologias contra o medo. Sociologias Plurais : Revista Discente do Programa de Pós-Graduação em Sociologia da Universidade Federal do Paraná [Em linha]. 3:2 (2015) 122-141. [Consult. 18 mar.

2022]. Disponível em WWW:<URL:
<https://revistas.ufpr.br/sclopr/article/view/64765/37692>>.

OLIVA, Diego Coletti ; PÁTARO, Carolina Ribeiro (2017) - Os usos e abusos do olhar : classificando corpos por trás das câmeras de videomonitoramento. Revista PsicoFAE Pluralidades em Saúde Mental [Em linha]. 6:2 (2017). [Consult. 18 jan. 2022]. Disponível em WWW:<URL:<https://revistapsicofae.fae.edu/psico/article/view/136>>.

OLIVEIRA, Erivan (2019) – Impacto do uso da inteligência artificial em sistemas de gestão empresarial no exercício da profissão contábil [Em linha]. [S.l.] : FAMAM. . [Consult. 18 mar. 2022]. Disponível em WWW:<URL:<http://famamportal.com.br:8082/jspui/handle/123456789/1576>>.

OSSAMU, Carlos (2021) - Gastos com Big Data e Analytics devem ultrapassar US\$ 215 bi este ano. Infor Channel [Em linha]. (17 ago. 21021). [Consult. 18 nov. 2021]. Disponível em WWW:<URL:<https://inforchannel.com.br/2021/08/17/gastos-com-big-data-e-analytics-devem-ultrapassar-us-215-bi-este-ano/>>.

OWEN, Mackenzie (2007) – Rethinking Knowledge Management. New York : Springer.

PANGILINAN, Erin ; LUKAS, Steve ; MOHAN, Vsanth (2019) – Creating Augmented & Virtual Realities. Sebastopol : O'Reilly Media.

PARKS, Lisa (2001) - Satellite views of Srebrenica : Tele-visibility and the politics of witnessing. Social Identities : Journal for the study of Race, Nation and Culture [Em linha]. 7:4 (2001). [Consult. 18 mar. 2022]. Disponível em WWW:<URL:<https://doi.org/10.1080/13504630120107728>>.

PERKIN, Neil ; ABRAHAM, Peter (2017) - Building the agile business through Digital Transformation. London : KoganPage.

POLITICS.CO.UK (2021) – Surveillance [Em linha]. [S.l.] : Politics.co.uk. [Consult. 18 mar. 2022]. Disponível em WWW:<URL: <https://www.politics.co.uk/reference/cctv/>>.

PORTUGAL. Leis, decretos, etc. (2021) - Lei de Organização da Investigação Criminal : Lei n.º 49/2008, de 27 de Agosto. PGDL – Procuradoria-Geral Distrital de Lisboa : Ministério Público [Em linha]. Lisboa : PGDL. [Consult. 18 mar. 2022]. Disponível em WWW:<URL:

https://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1021&tabela=leis&so_miolo=>.

RASMUS, Daniel (2017) - “O futuro mais provável é o da cibernética, da simbiose entre humanos e máquinas”. IT Insight [Em linha]. (15 dez. 2017). [Consult. 18 mar. 2022]. Disponível em WWW:<URL:<https://www.itinsight.pt/news/insight/o-futuro-mais-provavel-e-o-da-cibernetica-da-simbiose-entre-humanos-e-maquinas>>.

ROGERS, Ann ; HILL, John (2014) - Unmanned, drone warfare and global security. [S.l.] : PlutoPress.

ROQUE, Andre ; SANTOS, Lucas Braz Rodrigues dos (2021) - Inteligência Artificial na tomada de decisões Judiciais. Revista Eletrônica de Direito Processual [Em linha]. 22:1 (2021) 58-78. [Consult. 18 mar. 2022]. Disponível em WWW:<URL: <https://www.e-publicacoes.uerj.br/index.php/redp/article/view/53537/36309>>.

RUSSELL, Bertrand (2009) - The basic writings of Bertrand Russell. Edited by Robert E. Egner, Lester E. Denonn;

RUSSELL, Bertrand (s.d.) - Theory of knowledge [Em linha]. [S.l.] : MIA. [Consult. 18 mar. 2022]. Disponível em WWW:<URL:<https://www.marxists.org/reference/subject/philosophy/works/en/russell1.htm>>.

SATARIANO, Adam (2019) – Real-time surveillance will test the British tolerance for cameras. The New York Times [Em linha]. (15 Sep. 2019). [Consult. 18 mar. 2022]. Disponível em WWW:<URL:<https://www.nytimes.com/2019/09/15/technology/britain-surveillance-privacy.html>>.

SAWAYA, Márcia (1999) – Dicionario de Informatica e Internet [Em linha]. São Paulo : Edição Nobel. [Consult. 18 mar. 2022]. Disponível em WWW:<URL: <https://aeaveiro.pt/biblioteca/view/843/Dicionario%20de%20Informatica%20%26%20Int%20-%20Marcia%20Regina%20Sawaya.pdf>>.

SCHENGENVISAINFO (2019) - Greece Puts Tethered Aerostat in One-Month Trial Operation for Guarding Schengen Coast. SchengenVisalInfo [Em linha]. (30 Jul. 2019). [Consult. 18 mar. 2022]. Disponível em

WWW:<URL:<https://www.schengenvisainfo.com/news/greece-puts-tethered-aerostat-in-one-month-trial-operation-for-guarding-schengen-coast/>>.

SCHENGENVISAINFO (2020) - Frontex to Launch Pilot Project for Maritime Surveillance by Aerostat SchengenVisaInfo [Em linha]. (15 Sep. 2020). [Consult. 18 mar. 2022]. Disponível em WWW:<URL:<https://www.schengenvisainfo.com/news/frontex-to-launch-pilot-project-for-maritime-surveillance-by-aerostat/>>.

SEVERINO, Antônio (2014) – Metodologia do trabalho Científico. São Paulo : Cortez Editora.

SILVA, Germano Marques, (2008) - Curso de Processo Penal. 4.^a ed. revista e atualizada. Lisboa : Editorial Verbo. Vol. 2.

SOUSA, Marcelo (2001) – FOBOPOLE, O medo generalizado e a Militarização da Questão Urbana. [S.I.] : Bertrand Brasil.

SOUZA, Ribeiro (2016) – Proteção de Dados Pessoais. Brasília : Escola de Administração de Brasília.

TEAHAN, William (2010) - Artificial Intelligence : Agente Behaviour. London : Bookboon.com.

TEMPERTON, James (2015) - One nation under CCTV: the future of automated surveillance. Wired [Em linha]. (17 Ago. 2015). [Consult. 19 nov. 2021]. Disponível em WWW:<URL:<https://www.wired.co.uk/article/one-nation-under-cctv>>.

TOFFLER, Alvin (1971) - Future shock. 3rd printing. New York : Bantam Book.

UNITED KINGDOM. National Counter Terrorism Security Office (2020) – Guidance CCTV [Em linha]. [S.I.] : Gov.uk. [Consult. 14 mai. 2022]. Disponível em WWW:<URL:<https://www.gov.uk/government/publications/crowded-places-guidance/cctv>>.

VELÁQUES, Fernando ; CARBONERAS, Julia (2009) - Descontínua paisagem. In BEIGUEIMAN, Giselle [et al.] – Apropriações do (in) comum, espaço público e privado em tempos de mobilidade [Em linha]. São Paulo : Instituto Sérgio Motta. [Consult. 18 mar. 2022]. Disponível em WWW:<URL:http://www.hrenatoh.net/curso/textos/_artemov_port_.pdf>

YAN, Wei Qi (2019) - Introduction to Intelligent Surveillance : Surveillance Data Capture, Transmission, and Analytics. 3th ed. Cham : Springer.

ZAVRŠNIK, Aleš, ed. (2016) - Drones and Unmanned Aerial Systems. New York : Springer.

ZHAI, Yikui (2018) – Biometric Recognition CCB, A Novel Finger-Knuckle-Print Recognition. New York : Springer.

ZHANG, He (2018) - Biometric Recognition CCB, Hybrid Fusion Framework for Iris Recognition Systems. New York : Springer.

ZHOU, Jie (2018) – Biometric Recognition. New York : Edição Springer.

APÊNDICES

LISTA DE APÊNDICES

- Apêndice A** - Entrevista Dr. Manuel Anes
- Apêndice B** - Entrevista Dr. Pedro Clemente
- Apêndice C** - Entrevista Dr. Luís Elias
- Apêndice D** - Entrevista Dr. Manuel Faustino
- Apêndice E** - Entrevista Dr. Paulo Nicolau
- Apêndice F** - Entrevista Eng.º Bruno Tomé

APÊNDICE A

Entrevista Dr. Manuel Anes

Esta entrevista encontra-se subordinada ao tema «Quais os principais contributos da Inteligência Artificial para o processamento de imagens digitais a utilizar na segurança pública?» para a dissertação de mestrado.

Tem como objetivo estudar as nuances relativas à recolha de ocorrências policiais pelas Forças e Serviços de Segurança e pelos cidadãos, com o envio direto para uma central de tratamento de informações, tendo em vista catalogar a informação por um sistema de Inteligência Artificial em conjunto com analistas, de forma a obter-se um mapa nacional de incidências de perturbação da ordem pública, para o planeamento das ações de prevenção e reação policial.

A garantia dos direitos fundamentais obriga a que, se seja capaz de preservar os direitos, liberdades e garantias dos cidadãos e ao mesmo tempo agilizar o uso de meios disponíveis nos domínios da investigação criminal, prevenção criminal e reação policial para investigar e apurar a verdade material.

A participação de V. Exas é por demais importante para este estudo, atendendo a sua relevância como ator preponderante do nosso sistema de segurança pública.

Muito obrigado pela sua aceitação,

Data: 31/08/2021

Nome: Dr. José Manuel Anes

Grau: Perito superior de criminalista e professor universitário

Função: Laboratório da Polícia Judiciária

Presidente do OSCOT—Observatório de Segurança, Criminalidade Organizada e Terrorismo.

Atendendo a sua experiência e conhecimento policial:

1. Considera relevante para a prevenção criminal e reação policial, desenvolver um sistema de informações mais consistentes?

Indispensável, é evidente que necessitamos no âmbito da segurança, possuir meios que nos auxiliem a perscrutar de maneira mais eficaz, por exemplo a identificação de pessoas, a identificação de atividades criminais, a prevenção de atividades criminais,

por aquilo que me é dado a saber a Inteligência Artificial é um passo em frente para nos ajudar a resolver estes problemas de forma rápida.

No exército chamava-se NEPs Normas de Execução Permanentes o que permitiria ter-se um sistema de auxílio a decisão, como já vem sendo utilizado no Laboratório da Polícia Judiciária de forma que os agentes da cena do crime não falhem em nada.

1. Julga que a gestão dos recursos policiais podia ser incrementada com um cenário de informações mais assertiva para a manutenção da ordem e tranquilidade pública?

A IA é muito importante, existe já software de análise de informações, não direi qual o País, mas esse software utiliza a IA para um dado suspeito, saber que tipo de relações o suspeito teve nesse País ou noutros países, isso já se viu no caso de uma ação terrorista em França, a cerca de um ano, de seguida apurou-se que o homem tinha ligações até com gente em Portugal, a IA ajuda imenso, portanto isto é um passo em frente enorme.

Para além da identificação de pessoas, vai que uma multidão perceba que está aqui um individuo que está referenciado etc. são coisas poderosíssimas, eu acho que esse é o caminho para, já nem digo futuro, é o caminho presente.

2. Quais as principais etapas e ou tecnologias (e.g. IA) necessárias para uma inovação na recolha de dados numa força de segurança pública?

Em primeiro lugar mudar a mentalidade do agente ou inspetor. É fundamental, pois se ele continua agarrado ao lápis e papel e a máquina de escrever reage contra a inovação, ora a inovação é fundamental, poupa tempo, procede a um melhor arquivo de toda a informação que estiver a ser recolhida e pode guiar os comportamentos profissionais do agente no terreno, de forma muito importante.

Lembrando os primeiros microcomputadores *ZX Spectrum*, só depois vieram outros computadores mais poderosos, mesmo assim, houve muita gente do Laboratório da PJ que já com o *ZX Spectrum* faziam bases de dados muito interessantes, nós temos é de estar abertos a inovação e não sermos um entrave, isso é péssimo, é muito mau.

A IA possibilita melhorar a rapidez de acesso a informação, temos de começar a trabalhar já no presente e futuro.

3. Quais os principais contributos da IA para o processamento de imagens a utilizar na segurança pública?

Identificação de suspeitos é fundamental, a georreferenciação das ocorrências, como exemplo no caso de uma cidade ou freguesia onde há maior número de assaltos, embora se aconselhe a tratar estes dados de forma discreta para não criar pânico.

O Sistema de segurança interna já possui um bom software de georreferenciação, não sei se já tem os contributos da IA, mas já dava para funcionar e para além da georreferenciação, a identificação de suspeitos.

Presenciei num congresso em Montreal no Canadá em que a georreferenciação estava bastante avançada, eu por exemplo cheguei aos Estados Unidos e o aeroporto para além das impressões digitais, também permitia a identificação pelas iris, isto também é uma contribuição forte da IA, as conjugações de todos estes processos são fundamentais para identificação humana e sobretudo para identificação de suspeitos.

O software de análise de informações que referi com a integração da IA, a partir de fontes abertas, sem ser necessário a intervenção do Juiz, trata-se de um grande caminho, um caminho muito importante que nós estamos a encetar, mas que é indispensável, temos de ter uma justiça mais segura, mais certa, mais rápida e mais eficaz, isto é absolutamente indispensável.

Os contributos da ciência, a ciência é uma coisa boa, agora os conspiracionistas que não gostam da ciência, a ciência é muito importante, venha ela com os auxílios como a IA que é um grande auxílio, um grande contributo para segurança de todos nós.

4. Gostaria de alertar ou de acrescentar algum comentário contributivo para o objetivo geral do trabalho?

O objetivo geral do seu trabalho, é um excelente contributo, o mestrado não pode apenas olhar para coisas que sucederam, mas também para coisas que estão a chegar, como é a IA, dou-lhe os meus parabéns pelo facto de ser um tema muito bem visto, a IA tem um conjunto de aplicações ao nível da segurança enorme e muito desafiante.

APÊNDICE B

Entrevista Dr. Pedro Clemente

Esta entrevista encontra-se subordinada ao tema «Quais os principais contributos da Inteligência Artificial para o processamento de imagens digitais a utilizar na segurança pública?» para a dissertação de mestrado.

Tem como objetivo estudar as nuances relativas a recolha de ocorrências policiais pelas Forças e Serviços de Segurança e pelos cidadãos, com o envio direto para uma central de tratamento de informações, tendo em vista catalogar a informação por um sistema de Inteligência Artificial em conjunto com analistas, de forma a obter-se um mapa nacional de incidências de perturbação da ordem pública, para o planeamento das ações de prevenção e reação policial.

A garantia dos direitos fundamentais obriga a que, se seja capaz de preservar os direitos, liberdades e garantias dos cidadãos e ao mesmo tempo agilizar o uso de meios disponíveis nos domínios da investigação criminal, prevenção criminal e reação policial para investigar e apurar a verdade material.

A participação de V. Exas é por demais importante para este estudo, atendendo a sua relevância como ator preponderante do nosso sistema de segurança pública.

Muito obrigado pela sua aceitação,

Data: 15/09/2021

Nome: Pedro José Gomes Clemente

Grau: Superintendente-Chefe da PSP, doutorado

Função: Inspetor Geral na PSP, Docente Universitário

Atendendo a sua experiência e conhecimento policial:

1. Considera relevante para a prevenção criminal e reação policial, desenvolver um sistema de informações mais consistentes?

Estamos plenamente de acordo, é muito afirmativo, a informação hoje em dia é muito importante, a investigação criminal baseia-se sobretudo em informação, o que pressupõe dados trabalhados.

Muitas vezes quando são decididas as medidas de coação aplicadas, nomeadamente a prisão preventiva ou não, é muito importante, enfim incorporar toda essa informação, de forma que a magistratura possa tomar a sua decisão.

2. Julga que a gestão dos recursos policiais podia ser incrementada com um cenário de informações mais assertivo para manutenção da ordem ou tranquilidade pública?

Obviamente que sim, uma coisa é estar perante manifestações realizadas por entidades que já as fazem há muitos anos em que já são conhecidos os procedimentos, outra é quando estão organizações quase inorgânicas, ou seja, entidades com pouca estrutura em que não as conhecemos, e sobretudo hoje em dia é importante com os novos movimentos sociais que surgem por vezes com cariz violento, a preparação para evitar que isso aconteça é muito importante.

Há aqui um dado que é relevante, Sun Tzu na Arte da Guerra, tem uma declaração que é muito importante “não faças o jogo do adversário”, porque o adversário quer que se faça o seu jogo.

Muitas vezes as manifestações querem obter determinado tipo de resultados, isso passa por exemplo por quebrar as barreiras, por ocupar qualquer coisa, por obrigar a polícia a fazer uma carga mais forte, se nós obtivermos a informação devida, poderemos usar meios mais adequados, de contenção pacífica, como barreiras e deste modo contrariar o jogo do adversário.

A informação é uma boa ferramenta nesse sentido.

A analogia deste efeito com o futebol é como um defesa que passa o jogo a provocar o atacante adversário para provocar a expulsão e vice-versa, a informação permite jogar com isso.

3. Quais as principais etapas e ou tecnologias (e.g. IA) necessárias para uma inovação na recolha de dados numa força de segurança pública?

Sem comentários.

4. Quais os principais contributos da IA para o processamento de imagens a utilizar na segurança pública?

Hoje, a Polícia não passa sem Inteligência Artificial, tem de ser um modelo sistémico que integre as diversas plataformas e simultaneamente seja integrador, para que as bases de dados falem entre si, é preciso falarem, pensar em todos os sistemas de forma integrada, seja na observância da via pública, ou dentro de um estádio de futebol, até uma participação de um cidadão que fez uma denúncia anónima ou não, através de uma esquadra virtual.

É preciso incorporar principalmente os mais velhos, nestas novas tecnologias, para explorar esta nova informação.

Depois mete-se outro problema também, a montante, que é por exemplo nós fazermos a previsão do tipo de crime e vamos buscar os carteiristas todos, por hipótese ao sabermos que os carteiristas saem de Bogotá para irem fazer o verão em Roma, depois de tudo preparado, no entanto é preciso que o sistema judicial esteja alinhado com a operação, mas se o sistema judicial entra de férias no verão e é no verão que trabalham os carteiristas.

Podemos ter uma resposta tecnológica, mas, não ter uma resposta procedimental em outro órgão, como se sabe, quem apanha não julga, é necessário que as outras entidades também estejam preparadas para lidar com estes resultados, até do ponto de vista da linguagem, isto é muito importante, pois nós hoje estamos formatados para determinadas caixas de conhecimento (ex.: caixa jurídica), porém entra a caixa tecnológica e parece que estamos a falar línguas diferentes, ou seja é muito importante que quem está a incorporar o processo e assim como, quem recebe o produto saiba o que fazer com ele.

Isto é como comprar um Ferrari e não ter estradas para andar, por que está no meio do deserto.

O desafio é como preparar hoje, para tirar o melhor partido dessa integração.

5. Gostaria de alertar ou de acrescentar com algum comentário contributivo para o objetivo geral do trabalho?

APÉNDICE C

Entrevista Dr. Luís Elias

Esta entrevista encontra-se subordinada ao tema «Quais os principais contributos da Inteligência Artificial para o processamento de imagens digitais a utilizar na segurança pública? para a dissertação de mestrado.

Tem como objetivo estudar as nuances relativas à recolha de ocorrências policiais pelas Forças e Serviços de Segurança e pelos cidadãos, com o envio direto para uma central de tratamento de informações, tendo em vista catalogar a informação por um sistema de Inteligência Artificial em conjunto com analistas, de forma a obter um mapa nacional de incidências de perturbação da ordem pública, para o planeamento das ações de prevenção e reação policial.

A garantia dos direitos fundamentais obriga a que, se seja capaz de preservar os direitos, liberdades e garantias dos cidadãos e ao mesmo tempo agilizar o uso de meios disponíveis nos domínios da investigação criminal, prevenção criminal e reação policial para investigar e apurar a verdade material.

A participação de V. Exas é por demais importante para este estudo, atendendo a sua relevância como ator preponderante do nosso sistema de segurança pública.

Muito obrigado pela sua aceitação,

Data: 22/09/2021

Nome: Luís Manuel André Elias

Grau: Superintendente da PSP e Doutorado

Função: Diretor do Departamento de Operações da PSP e docente universitário

Atendendo a sua experiência e conhecimento policial:

1. Considera relevante para a prevenção criminal e reação policial, desenvolver um sistema de informações mais consistente?

Trata-se de um aspeto muito relevante, é uma necessidade e estamos a caminhar nesse sentido, em caso de furto ou de roubo, poder-se na hora transpor a ocorrência para o sistema de informações, este processo da mobilidade é um recurso em que estamos mais avançados na área do trânsito, na parte criminal, estamos em vias de implementação, tão logo consigamos apetrechar as equipas com tabletes.

Alguns nichos já operam nesse sentido, uma das nossas necessidades é tornar este fluxo de informação muito mais dinâmico, possuímos um grande repositório de informação, que vem sendo alimentado a cerca de duas décadas.

O sistema estratégico de informação da PSP, está num processo contínuo de atualização, a mobilidade é uma mais-valia, que permite, de uma forma muito célere, recolher informação em tempo real, para potenciar gatilhos na base de dados, de forma a gerar alertas imediatos para o terreno, ao que estes na presença de indivíduos suspeitos ou procurados possam ser identificados (ex. com mandado de captura, etc.).

Há aqui diversas mais-valias que permitirão maior imediatismo na análise da informação e respostas mais rápidas, de forma a ganhar eficiência e a eficácia.

2. É de opinião que a gestão dos recursos policiais podia ser incrementada com um cenário de informações mais assertiva para a manutenção da ordem e tranquilidade pública?

O policiamento preditivo consiste em procurar antecipar o cometimento de perigos, atualmente temos ferramentas que podem fazer isso, o problema é que a crescente automatização, o *big data*, a correlação entre bases de dados, a georreferenciação, criam novas oportunidades, hoje já é possível analisar tendências de locais, como hotspots, ou sejam locais geográficos onde há uma grande concentração de crimes.

O mais importante nisto tudo, é a capacidade de através do *big data* analisar tendências a de longo prazo.

Por hipótese, se todas as sextas-feiras no Rossio houvesse um conjunto de roubos por esticção, pelos mesmos dois suspeitos, pois as características apodas pelas vítimas são semelhantes, em três meses torna-se uma tendência, o que significaria que na sexta-feira seguinte, se poderia organizar uma ação policial para capturar os suspeitos em flagrante delito.

Esta é uma vantagem clara que a análise de dados criminais, pode trazer para a parte mais operacional da polícia, na perspetiva mais reativa, assim como na perspetiva da investigação criminal, onde poderá permitir a confrontação de suspeitos, em cenários de indivíduos que são detetados numa cidade, mas, estão a atuar em outra, a descrição das vítimas sobre as ocorrências, em termos de características, (forma de vestir, estatura, etc.), estas descrições do ponto de vista analítico podem ser muito importantes

para no meio da panóplia de dados, consigamos identificar esses suspeitos, noutras ocorrências que sejam reportadas.

Isto é muito útil, pois permite criar vantagens nas três vertentes, da prevenção criminal, da investigação criminal e da ordem pública.

3. Quais as principais etapas e ou tecnologias (e.g. IA) necessárias para uma inovação na recolha de dados numa força de segurança pública?

A questão de fundo é até que ponto os Estados e ou os cidadãos estão dispostos a prescindir de alguns direitos, é muito mais fácil o desenvolvimento destas tecnologias e a sua aplicação prática em regimes políticos menos democráticos que nos democráticos.

Há um conjunto de garantias nos estados de direito democráticos que de alguma forma criam obstáculos à aplicação prática de algumas dessas tecnologias, tendo em conta os atuais quadros legais em vigor, os regulamentos europeus de proteção de dados, etc.

No entanto, as empresas tecnológicas continuam o seu desenvolvimento imparável, haverá um momento em que as tecnologias se alinharão a realidade, isso já acontece todos os dias, em vários âmbitos da nossa vida pelas ferramentas que vão sendo criadas e difundidas na vida prática, tais como drones, sistemas de vídeo e vigilância, a análise da human intelligence, há um conjunto de uma vasta panóplia de ferramentas que vão impondo a realidade.

A questão de fundo, é que as entidades públicas dos países têm de criar mecanismos de regulação e controlo, sob pena de, se estas tecnologias estiverem somente na mão de alguns privados, e não na das instituições, sejam elas policiais ou outras, estas ferramentas poderem ser utilizadas para fins que não os previstos na lei (nomeadamente interesses privados, comerciais, chantagens políticas e etc.).

A ausência de regulação e controlo constitui um risco, pois a tecnologia avança mais rapidamente que a lei, portanto os estados com uma decisão política mais flexível, mais célere, que se adaptam mais rapidamente, podem contaminar os outros mais tradicionalistas.

A nível da vídeo vigilância nos espaços públicos, havia muitos obstáculos a cerca de 20 anos, hoje já largamente aplicada nos países ocidentais e não ocidentais em Portugal já temos muito mais locais a serem objeto de sistemas de vídeo vigilância em espaço público.

A evolução tecnológica é bem-vinda, mas, também deve haver alguma vigilância por parte do cidadão, este não pode abdicar dos seus direitos em prole de mais segurança, convinha que o equilíbrio necessário entre liberdade e segurança seja o mais balanceado possível, viver em sociedades assépticas e seguras, corre-se o risco de ver os direitos individuais serem devassados pelas diversas entidades.

4. Quais os principais contributos da IA para o processamento de imagens a utilizar na segurança pública?

A tecnologia dá-nos grandes perspetivas de identificar suspeitos, potencia o combate ao crime organizado e violento, há sistemas de reconhecimento facial, deteção de padrões e outros, implementados em alguns países.

Houve já muitos sucessos fruto dessa tecnologia, já foram evitados atentados porque os sistemas de vídeo vigilância, tinham acoplados software que detetam desvios ao padrão, o caso de um carro estacionado em local proibido em hora estranha, leva a que o centro de comando e controlo, desencadeie para lá meios para averiguar as razões do carro estar em local indevido, e neste caso em concreto as averiguações detetaram explosivos, isto aconteceu na cidade de Nova Iorque, na times square.

A capacidade adicional que há de detetar situações suspeitas, que se podem confirmar ou não, também se aplica a indivíduos, outra utilidade grande está na deteção de bagagens abandonadas em aeroportos, estações de caminho de ferro ou outras, para alertar e desencadear o processo da ação humana, na verificação desses alertas que podem corresponder a um agente explosivo que ali foi plantado dolosamente.

Um aspeto que não nos podemos esquecer, a tecnologia por si não pode ser aplicada em detrimento da human intelligence, que esta tecnologia não faça a polícia abandonar o contato com as comunidades, com os informadores, senão correremos o risco de ter somente uma perspetiva assética da realidade.

Quando temos forças a operar drones em países longínquos, sentados no seu país natal a milhares de quilómetros de distância, eles não estarão a cheirar a realidade,

independentemente da eficácia, o que por vezes acontece, é termos muitos danos colaterais no resultado.

É importante que esta evolução tecnológica seja acompanhada na continuidade da aposta com trabalho no terreno, que até ver são os humanos a fazer, mesmo antevendo um enorme desenvolvimento tecnológico, não devemos abandonar a human intelligence.

6. Gostaria de alertar ou de acrescentar algum comentário contributivo para o objetivo geral do trabalho?

APÊNDICE D

Entrevista Dr. Manuel Faustino

Esta entrevista encontra-se subordinada ao tema «Quais os principais contributos da Inteligência Artificial para o processamento de imagens digitais a utilizar na segurança pública?» para a dissertação de mestrado.

Tem como objetivo estudar as nuances relativas a recolha de ocorrências policiais pelas Forças e Serviços de Segurança e pelos cidadãos, com o envio direto para uma central de tratamento de informações, tendo em vista catalogar a informação por um sistema de Inteligência Artificial em conjunto com analistas, de forma a obter-se um mapa nacional de incidências de perturbação da ordem pública, para o planeamento das ações de prevenção e reação policial.

A garantia dos direitos fundamentais obriga a que, se seja capaz de preservar os direitos, liberdades e garantias dos cidadãos e ao mesmo tempo agilizar o uso de meios disponíveis nos domínios da investigação criminal, prevenção criminal e reação policial para investigar e apurar a verdade material.

A participação de V. Exas é por demais importante para este estudo, atendendo a sua relevância como ator preponderante do nosso sistema de segurança pública.

Muito obrigado pela sua aceitação,

Data: 23/08/2021

Nome: Manuel José Serrano Faustino

Grau: Subinspetor, Licenciado em direito

Função: Chefe da Divisão de Investigação Criminal da Polícia Marítima

Atendendo a sua experiência e conhecimento policial:

1. Considera relevante para a prevenção criminal e reação policial, desenvolver um sistema de informações mais consistentes?

A informação centralizada em cada OPC, pode gerar informação especulativa, muitas vezes por questões culturais, o próprio órgão não a disponibiliza em tempo real, o ideal

quando se fala em informação centralizada seria um sistema único para todas as polícias.

Com métricas de acesso únicas e claras, o que significaria manter o segredo de justiça para investigações paralelas, poderia haver nos sistemas um alerta para essa existência e o seu acesso ser feito apenas pelas vias legais do titular desse inquérito, obter tudo isto em tempo real, por um sistema de informação centralizado, mas, tendo em atenção as próprias rotinas internas de cada órgão.

2. Julga que a gestão dos recursos policiais podia ser incrementada com um cenário de informações mais assertivo para manutenção da ordem ou tranquilidade pública?

Penso que sim e tem de ser, me parece que estamos atrasados nesta matéria.

A gestão dos recursos humanos é a coisa mais importante, não importa o cenário, a polícia tem uma preocupação, cumprir e fazer cumprir a lei, garantir os direitos e liberdades das pessoas, a segurança das pessoas e bens.

A gestão dos recursos utilizando IA, permite-nos disponibilizar os meios necessários para cada momento real, porque temos informação presencial, é possível hoje em dia que alguém que esteja no centro de comando e controlo , numa situação de risco , por exemplo um evento desportivo, um incidente num transporte público, seja o tipo de ação que for, mesmo a mais violenta, é possível alguém que esteja no CCC efetivo, apenas com uma comunicação que se efetua hoje em dia com um telemóvel, através de uma imagem do controlo da situação a distância, com essa imagem consegue disponibilizar os recursos policiais que efetivamente sejam capazes de dominar a situação, para poder ter domínio da situação, a imagem do que se está a passar em tempo real é determinante, a partir daí, não há dúvidas de que estamos a quem desse cenário.

As polícias normalmente estão a correr atrás do acontecimento, no entanto esta assimetria é um problema legal, normalmente o legislador vai atrás do acontecimento de forma reativa.

A salvaguarda dos direitos, liberdades e garantias, imaginemos a situação em voga, as câmaras de vídeo vigilância, a utilização de drones, utilização das bodycams a exemplo, é inevitável, mas, temos uma limitação legal em termos de proteção de dados, da

proteção de imagens e aqui temos um choque, que é a necessidade coletiva de proteção e a necessidade individual daquela pessoa em concreto.

Ainda bem que esse trabalho é feito, na minha perspetiva policial, não tenho dúvidas de que havendo um controlo efetivo sobre os CCC das polícias, garantida com uma fiscalização correta, as entidades de fiscalização da proteção de dados, numa ação muito incisiva, que a sociedade teria tudo a ganhar, primeiro porque temos a garantia de que aquela preservação de imagem fica, a sua obtenção é no espectro da segurança e da liberdade, se estiver a filmar uma pessoa, não estou a retirar a imagem, eu retiro a imagem quando uso essa gravação para fins que não são lícitos, por isso às pessoas que passam na sua vida e que ficarão filmadas em arquivo, deverá ser garantida que essa imagem, seja removida no tempo quando se verificar que ela não trás nenhum benefício para a segurança.

Agora, mais uma vez é que nas nossas sociedades estão a correr sistematicamente atrás do prejuízo, atrás do incidente e atrás muitas vezes não resolve, porque acabamos por perder muita da capacidade de garantir a segurança, porque há a retração da sociedade, essa não disponibilidade da sociedade, para atribuir em tempo os meios tecnológicos e de inteligência que já seriam admissíveis nesta altura do campeonato.

Garantidamente estaríamos numa fase de muito mais segurança, se esses meios tecnológicos já admissíveis estivessem ao serviço da polícia na liberdade da ação, logicamente com a ponderação necessária, devido ao resguardo da salvaguarda da dignidade da pessoa humana e do direito a confidencialidade.

A segunda vertente, é a individualização do agente policial que se encontra no terreno, efetivamente, o chamado polícia de giro, que são a grande massa das ações policiais, que fazem o trabalho de proximidade, o primeiro elemento de esquadra, piquete, posto que é disponibilizado para as situações e é o primeiro a chegar, é o mais mal preparado, não por culpa própria, mas é quase impossível dar formação a uma agente que anda na rua, quando está na rua não está em formação.

Havendo a disponibilidade no CCC em que nós tivéssemos a perceção clara do acontecimento do momento, seria possível encaminhar o agente sobre o que deve fazer, através do telemóvel com a checklist.

A checklist é importante, se nós catalogarmos às situações, isto acontece muito por exemplo com os Estados Unidos, os americanos fazem muito a catalogação para saber quando há um incidente, o que correu mal, para que não volte a acontecer.

Se utilizarmos a IA que temos hoje disponível, através dos meios informáticos, bastaria o agente clicar a tipologia do incidente e se tivermos uma checklist, além do controlo, é um auxílio, porque o agente a partir daí, perante o stress da situação, perante a ação, o ser humano tende a reagir de forma diferente a cada situação, posso ter um indivíduo calmo que reage com ponderação ou ter um outro indivíduo que não reage tão bem, que reage sobre brasas, o stress é normal, se tiver um alerta com ele e o possa dizer nesta situação, para ter atenção a determinadas situações, observar estes e estes pontos, as maiores falhas, uma checklist para diminuir o erro na obtenção de prova por exemplo, não é repetitivo, as situações não se repetem na vida.

Para eliminar o erro no âmbito por exemplo da obtenção de prova, o agente estaria numa fase diferente pois estaria a obter um treino dentro do próprio trabalho, seria uma situação em que o vai mecanizando e acabaria por ser uma formação no momento da ação.

Esta parte da gestão do recurso e da formação virtual é por demais importante, pois, todos os meios tecnológicos ao dispor poderiam ser utilizados mais corretamente, para potenciar o homem.

3. Quais as principais etapas e ou tecnologias (e.g. IA) necessárias para uma inovação na recolha de dados numa força de segurança pública?

Há toda a necessidade de dar ao agente formação, de forma, a ser cada vez mais capaz.

A necessidade da formação do homem é importante, a experiência passada no tempo do Windows 3.11 ainda em inglês nos anos 90, vivida por mim com alguns colegas mais idosos à época, em que na mudança da máquina de escrever para o computador, o que foi um grande avanço, agora imagine o avanço para alguém que deixou de substituir o papel quando se fazia um erro, pois um relatório com quatro ou cinco páginas, quando se estraga uma página por vezes era necessário fazer tudo de novo, quando o chefe corrigisse, frequentemente tínhamos que voltar a datilografar as correções.

A evolução histórica para o computador, veio facilitar todo este processo, os colegas a época envaidecidos com o uso do computador, um único para toda a gente, em que

cada um tinha sua disquete e fazia já os seus relatórios, entretanto o Microsoft Windows fez a sua evolução histórica e passa a estar disponível em português, com correção de erros.

Esta evolução, criou um retrocesso no grupo, pois ninguém queria trabalhar com a versão em português, porque ninguém sabia o que aquilo queria dizer, passámos de uma linguagem em inglês em que mesmo sem saber falar a língua existiam automatizações, porém o programa em português não fazia sentido, pois na nossa língua não se sabia como usar o programa, de tal modo que alguns queriam voltar para a maquina de escrever, isto foi ultrapassado com as explicações que tivemos de dar aos colegas.

Este pequeno exemplo, espelha bem o impacto da tecnologia e a necessidade de formação.

A principal etapa é a formação das pessoas, o problema é que quando se está em formação não se está no terreno a operar e a tecnologia vai novamente ajudar, pois com uma solução desta natureza, que dê inputs, deixa de haver a necessidade de estar muitas horas ou grandes momentos nas salas de aulas para este fim.

A recolha de dados deverá ser centralizada, obtermos toda a massa de disponibilidade técnica e ao mesmo tempo acompanhar com legislação, neste momento as principais etapas são dar um salto na legislação, para capacitar o uso de mais tecnologia na recolha de dados com instrumentos legais adequados.

A questão das imagens o legislador terá de adequar a parte legal, para poder dotar as policias de instrumentos legais, capazes de poderem usar na plenitude as tecnologias disponíveis.

Por exemplo, constatamos uma inadaptação que decorre eventualmente da capacidade financeira, tecnológica, mas também a alteração a lei penal de 2007 e 2008 possibilitou largar a escrita nos interrogatórios, pois os interrogatórios passaram a poder ser gravados digitalmente em sede judicial e também em sede policial.

No entanto, no âmbito da violência doméstica e dos crimes contra crianças, somente as unidades dedicadas estão a fazer essa gravação.

A produção do auto de interrogatório por escrito, por vezes o seu sentido pode ficar deturpado, pela simples aplicação de uma vírgula, e o interrogado ao assinar estará a dar força a uma declaração que está deturpada pela aplicação da vírgula, em contrapartida se o interrogatório for produzido utilizando a tecnologia que já esta disponível em lei, ao gravar-se a imagem, possibilita inclusivamente ver comportamentos e perceber o alcance da declaração de forma genuína.

Neste exemplo já existe legislação a permitir, mas, os aplicadores da lei não estão a acompanhar a sua aplicação.

Na resposta a uma ocorrência, quem chega ao local necessita de se inteirar do que se passou, para poder documentar, fotografar, etc., se for possível ouvir pessoas logo no local, ou outras situações, através dos meios informáticos existindo essa capacidade de forma segura, isto possibilita datar, documentar um incidente e essa prova, a lei hoje já permite em determinadas situações recolher imagens sem se fazer anunciar, mas há necessidade de autorização pelo controlo judicial.

A função da polícia é o auxílio aos órgãos de justiça, para fazer cumprir a lei, a utilização dos meios tecnológicos é fundamental, possibilita documentar de uma forma material, mais eficaz e que permita ao julgador, mais tarde, ter uma perceção plena dos factos, e para isso os meios tradicionais de recolha de prova documental, atualmente, uma imagem pode ser de uma verdade material inquestionável, necessitamos de expurgar o complexo para podermos usar os meios informáticos.

O reconhecimento facial, a análise de vestígios lofoscópicos, recolhidos por telemóvel e com a possibilidade de ligar remotamente para validar, para quem está no local da ocorrência, é de um potencial indiciário para a investigação, possibilita determinar o historial dos envolvidos, isto só será possível tão logo o legislador assim o permita.

O passo para a centralização dos dados numa plataforma única e colaborativa, para permitir disponibilizar dentro das funções de cada órgão a informação existente.

A maximização do controlo de acesso à plataforma centralizada, é pela análise da pegada digital que cada um deixa no sistema, permite auditar a informação disponibilizada para cada utilizador.

Por exemplo na presença de um incidente como um furto local, o perito no terreno pela análise em tempo real de dados lofoscópicos, ao invés de ter de os trazer para

laboratório e a posterior fazer o expediente, e depois a verificação, se tiver acesso remoto em tempo real, ainda que de forma preliminar, consegue-se reunir de imediato elementos indiciários, seja para a triagem para separar quem funciona no local e quais são os elementos estranhos, de seguida com a informação da plataforma centralizada, estabelece-se de imediato, se estamos perante alguém que já vem sendo procurado e deste modo possibilita ter um indicador para a investigação, esta pode ser uma das vantagens de aplicar a tecnologia, com ganho temporal enorme.

A questão que se coloca é se estamos preparados em termos legais para se poder dar este salto para acompanhar a tecnologia e ao mesmo tempo garantir a liberdade das pessoas, como sendo o elemento mais importante

4. Quais os principais contributos da IA para o processamento de imagens a utilizar na segurança pública?

O principal contributo é ser mais um fator para garantir a segurança em tempo real, vem maximizar a capacidade operacional.

Uma CCC, ao utilizarmos a IA, as capacidades tecnológicas na sua maximização, conseguiremos programar e fazer mais e melhor com os recursos disponíveis.

Por exemplo a utilização de CCTV em zonas de risco, como recintos desportivos, com a recolha das imagens, poder-se em detalhe verificar a ação de um individuo ou grupo relacionado com um incidente grave, poder-se identificar quem fez o quê?

O principal contributo da IA na investigação é mitigar o erro, reduzir ao mínimo admissível o erro humano.

Num interrogatório, ao ter a tecnologia ao seu dispor, o agente estará mais liberto, sem barreiras entre ambos, sem mesas, sem cadeiras, pois cada vez que se está a escrever é uma situação de conflito para o interrogado, a gravação digital permite diminuir o erro.

O acesso em tempo real para verificar dados, traduz-se na diminuição do tempo de aplicação da justiça, ao diminuir o erro, estamos a dar a capacidade de o investigador fazer a sua análise, correlação e síntese, maximização da capacidade e a justiça na aplicação do direito.

O legislador ao criar restrições está no pressuposto da preservação da pessoa humana, na legalidade dos factos, na defesa dos visados, mas na verdade pode estar a fazer o

contrário, porque se se aplicar a justiça fora do tempo, já se estiverem legalizados os meios tecnológicos poderemos de uma forma normal ter uma justiça mais célere.

Isto é muito importante, para se fazer justiça, quando não se utilizam os meios tecnológicos por força das restrições, normalmente, teremos mais dificuldades em fazer justiça.

Por exemplo quando alguém jovem com 18 anos numa noite de cabeça perdida, por consumo de álcool ou estupefacientes passa por alguém a levantar dinheiro no Multibanco e por falta de dinheiro, assalta esse individuo, inicia-se uma investigação que vai demorando tempo e ao fim de cinco anos consegue-se identificar o suspeito, neste espaço de tempo o jovem terminou a faculdade, já tem o seu emprego, nunca mais esteve envolvido em atividades criminosas.

Este tipo de cenário, vai fazer sofrer alguém que estaria ressocializado, mas, que por força da lentidão da justiça, ao ter demorado muito tempo a investigar, fez com que não fosse condenado a época, mas sim, cinco ou mais anos depois, isso não é justiça, porque se o suspeito se ressocializou, refez a sua vida, vamos condená-lo por algo que ele foi num passado longínquo e não por aquilo que é no presente, isto pode dar origem a uma injustiça.

Se a pessoa refez a sua vida, mas, vai em função da condenação ser privada de liberdade, depois de cumprir, estarão criadas as condições, para voltar ao que já fez no passado, deste modo, em vez de ter resolvido um desvio social, no final teremos criado um problema para sociedade.

Se no momento da investigação tivéssemos os meios tecnológicos de câmaras, a localização do telemóvel do suspeito com precisão do local, poder-se-ia ter enviado este para justiça em tempo oportuno.

Quanto mais avançados forem os meios tecnológicos disponíveis para os aplicadores da lei (polícia, ministério público, tribunais), quanto mais tecnologia houver disponível, mais aptos estaremos para aplicar a lei e fazer justiça.

Todos estes contributos tecnológicos servem para melhorar a sociedade no seu todo, de modo que as correções sejam aplicadas no momento certo.

No contexto europeu, por se terem suprimido as fronteiras internas e atendendo a que cada estado tem a sua própria política de segurança interna, os protocolos e a colaboração entre estados não chegam para o controlo, é necessário colocar a tecnologia ao serviço da União Europeia, independentemente das polícias que existam, quando estamos perante um criminoso no contexto europeu no qual os estados não são estanques em termos de circulação de pessoas e bens, mas, são estanques em termos de aplicação de justiça.

A inteligência artificial é importante porque potência, no entanto é importante que os interlocutores falem todos a mesma linguagem.

A exemplo, em tempos estivemos num evento na Finlândia com -21º Celsius, no entanto no encerramento, estava um dia um pouco ensolarado e com a temperatura de -5º Celsius e a responsável da Finlândia agradeceu porque os Portugueses teriam levado o sol para a Finlândia,

No discurso de encerramento o signatário português referiu que não sabia como começar o seu discurso de encerramento, então referiu, “aproveitando a sua deixa, de-me aqui um input grande, a importância de falarmos a mesma linguagem, que é o que nós procuramos, através da troca de informações, termos uma linguagem comum”, é muito importante para a IA, quando se utilizam meios tecnológicos, diz ele “se ligasse agora para minha casa e dissesse a minha mulher que na Finlândia esta um tempo maravilhoso, utilizando as mesmas palavras que referiu, a minha mulher iria dizer estão 20º ou 30º nesse sitio”, ou seja estamos todos a falar na mesma língua, o Inglês, mas não estamos a falar a mesma linguagem.

Os principais contributos na utilização dos meios tecnológicos, rapidez, separação, formação, capacidade de comando e controle, no espectro nacional entre as várias forças e UE entre os vários Países e as suas forças, o determinante é definir uma linguagem comum.

A tecnologia é extremamente importante, a IA será certamente importante, mas, as premissas de ação, de alertas e tudo o mais, têm de ser comuns, ser perceptíveis, ser entendíveis, temos de falar a mesma linguagem, para potenciar o entendimento entre todos.

5. Gostaria de alertar ou de acrescentar algum comentário contributivo para o objetivo geral do trabalho?

Quando se fala em aplicar tecnologia às forças de segurança, temos pelo menos dois impedimentos, sendo o primeiro o aspeto legal, o segundo a carga da doutrina interna, por outro lado, na aplicação da IA um desafio importante a considerar é o impacto do aumento ou diminuição do poder em alguns atores da segurança, com reflexos na resistência a mudança.

APÊNDICE E

Entrevista Dr. Paulo Nicolau

Esta entrevista encontra-se subordinada ao tema «Os principais contributos da Inteligência Artificial para o processamento de imagens digitais a utilizar na segurança pública.» para a dissertação de mestrado.

Tem como objetivo estudar as nuances relativas à recolha de ocorrências policiais pelas Forças e Serviços de Segurança e pelos cidadãos. Pretende ainda estudar a pertinência do envio direto para uma central de tratamento de informações, tendo em vista catalogar a informação por um sistema de Inteligência Artificial (IA) em conjunto com analistas, de forma a obter um mapa nacional de incidências de perturbação da ordem pública, para o planeamento das ações de prevenção e reação policial.

Sabendo-se que a garantia dos direitos fundamentais obriga a que se seja capaz de preservar esses mesmos direitos, liberdades e garantias dos cidadãos e ao mesmo tempo agilizar o uso de meios disponíveis nos domínios da investigação criminal, prevenção criminal e reação policial para investigar e apurar a verdade material, é determinante aprofundar o estudo deste tema

Assim, a participação de V.Ex.^a é fulcral para este estudo, atendendo a sua relevância como ator preponderante do nosso sistema de segurança pública.

Muito obrigado pela sua colaboração e contributo para o avanço do conhecimento.

Data: 05/04/2021

Nome: Paulo Alexandre Nicolau

Grau: Inspetor coordenador superior e doutorado

Função: Diretor regional do SEF Madeira, docente universitário

1. Considera relevante para a prevenção criminal e reação policial, desenvolver um sistema de informações mais consistentes?

Em Portugal existem sistemas de informações consolidados, no quadro das FSS, os quais podem a todo o tempo e sempre que se justifique serem melhorados para uma melhor adequação à realidade portuguesa.

2. Julga que a gestão dos recursos policiais podia ser incrementada com um cenário de informações mais assertiva para a manutenção da ordem e tranquilidade pública?

Os cenários construídos com base em informações já têm presentemente uma elevada relevância na gestão eficaz dos recursos policiais, para a manutenção da ordem e tranquilidade pública.

3. Quais as principais etapas e ou tecnologias (e.g. IA) necessárias para uma inovação na recolha de dados numa força de segurança pública?

Ao nível da recolha de dados numa força de segurança pública, no quadro da legislação nacional e europeia, naturalmente a intervenção da Comissão Nacional de Proteção de Dados em termos regulatórios.

4. Quais os principais contributos da IA para o processamento de imagens a utilizar na segurança pública?

No âmbito da segurança pública, considero que um dos eventuais contributos poderá ser ao nível do reconhecimento facial, depois de devidamente dirimidas as questões inerentes à salvaguarda dos direitos, liberdades e garantias dos cidadãos.

5. Gostaria de alertar ou de acrescentar com mais algum comentário para o objetivo geral do trabalho?

O objetivo geral do trabalho é da exclusiva responsabilidade do candidato, nada tendo a acrescentar.

APÊNDICE F

Entrevista Eng.º Bruno Tomé

Esta entrevista encontra-se subordinada ao tema «Quais os principais contributos da Inteligência Artificial para o processamento de imagens digitais a utilizar na segurança pública?» para a dissertação de mestrado.

Tem como objetivo estudar as nuances relativas à recolha de ocorrências policiais pelas Forças e Serviços de Segurança e pelos cidadãos, com o envio direto para uma central de tratamento de informações, tendo em vista catalogar a informação por um sistema de Inteligência Artificial em conjunto com analistas, de forma a obter-se um mapa nacional de incidências de perturbação da ordem pública, para o planeamento das ações de prevenção e reação policial.

A garantia dos direitos fundamentais obriga a que, se seja capaz de preservar os direitos, liberdades e garantias dos cidadãos e ao mesmo tempo agilizar o uso de meios disponíveis nos domínios da investigação criminal, prevenção criminal e reação policial para investigar e apurar a verdade material.

A participação de V. Exas é por demais importante para este estudo, atendendo a sua relevância como ator preponderante do nosso sistema de segurança pública.

Muito obrigado pela sua aceitação,

Data: 05/08/2021

Nome: Bruno Tomé

Grau: 1o. Sargento, Engenheiro Informático

Função: Analista de Cibersegurança da Guarda Nacional Republicana

Atendendo a sua experiência e conhecimento policial:

- 1. Considera relevante para a prevenção criminal e reação policial, desenvolver um sistema de informações mais consistentes?**

Depende.

Vai ter várias vantagens como desvantagens.

Sim, tem toda a lógica que sejam desenvolvidos numa forma mais consistente, porque, muitas vezes aquilo que está desenvolvido, já não está atualizado, nem se enquadra a realidade atual.

O que acontece é termos vários sistemas de informação, mas muitos deles não são atualizados, não estão enquadrados a realidade de quem trabalha a nível criminal, nem na prevenção, nem na forma como nós estamos a atuar.

Por isso, convinha também ter um sistema, que se fosse atualizando e tivesse um enquadramento legal, porque, muitas vezes ele foi desenvolvido há a muitos anos e nunca acompanhou a evolução tanto a nível criminal de procedimentos, como a nível legal e muitas vezes, o que está lá não corresponde a realidade do que está a ser feito.

Por isso, seria uma mais-valia para quem está no terreno, ter já alguma informação correta, precisa e concisa para poderem atuar e muitas vezes cobrir algumas lacunas que existam na lei.

Pela minha experiência profissional, quem está no campo, no terreno, toma conta de diversos assuntos, tanto a violência doméstica, um furto, um roubo, um acidente rodoviário, ou um assalto a mão armada, por exemplo, coação e muitas vezes uma pessoa sai de uma situação e vai para outra e se tiver algo que o ajude, que o apoie, torna-se tudo muito mais fácil, porque, é um leque tão grande, que quem está fora tem de saber, a nível criminal, de leis, de procedimentos, se tiver uma informação algo que o ajude, neste caso tem aqui estes tópicos e é assim que se deve atuar, e deve-se guardar ou salvaguardar esta prova para ser legal ao nível do tribunal judicial.

O que se vê é que não há nada, as vezes o que há, está desenquadrado da realidade dos procedimentos que as pessoas têm que aplicar no terreno e a nível criminal quando recolhem provas, convinha ter um sistema ao nível de informações, que fosse atualizado e que fosse mais adequado na ajuda a prevenção de quem está no terreno.

2. Julga que a gestão dos recursos policiais podia ser incrementada com um cenário de informações mais assertivo para manutenção da ordem ou tranquilidade pública?

A gestão dos recursos humanos ou recursos policiais é muito complicada, é assim, porque, nos últimos anos neste caso tanto a GNR como a PSP e outras forças policiais, cada vez têm menos recursos humanos.

E a informação claro, se fosse mais precisa e assertiva, talvez conseguissem canalizar esses recursos para as áreas onde eles poderiam atuar ao nível de criminologia.

Se a informação for mais assertiva, tem toda a lógica, em vez dos recursos estarem mais espalhados, eles poderiam estar com um foco mais assertivo com aquilo que é, se a informação fosse mais concreta.

Por vezes a informação que é recolhida, é muito vaga, muito ampla, o que dificulta neste caso a alocação de recursos humanos, uma vez que já há um défice.

Se ela fosse mais assertiva, mais concisa, deste modo os recursos humanos poderiam ser canalizados de forma mais assertiva nas situações locais ao nível da prevenção.

3. Quais as principais etapas e ou tecnologias (e.g. IA) necessárias para uma inovação na recolha de dados numa força de segurança pública?

Depende do tipo de dados que vamos recolher, se são conteúdos informáticos ou provas físicas de algum crime.

Na visão da ajuda futura, no caso dos acidentes rodoviários, deveria existir já uma plataforma, que permitisse colocar logo tudo ao nível de quantos feridos, graves, ligeiros, automaticamente, carregar-se sem recorrer ao papel, e depois comunicar através de tablete onde os agentes preenchessem os campos principais, vítima, faixa etária, masculino, feminino, estado grave, ligeiro, tipo de acidente, se foi com vários veículos, se resultou em mortos ou não, isso ajudava bastante, para já facilitava ao nível do trabalho, e também permitia ter toda estatística, de quantos acidentes rodoviários ao nível nacional, neste caso por trimestre ou fase do ano.

A nível de crimes também é interessante, por exemplo, ter este tipo de tecnologia, acho que a tablete é ideal para o terreno, ajudava para já a tirar fotografias, preservava os indícios, e seria mais fácil, podiam gravar qualquer coisa ao nível de prova, só que isso, teria de ser válido em tribunal, o que é complicado pois muitas vezes não são considerados.

Em cenários em que uma porta foi rebentada, está toda partida, eles poderiam tirar fotografias ou filmar a registar esse fato, possibilitaria a quem estivesse a reconstruir esse fato, era mais fácil entender como foi feito o assalto, ou porque assaltaram aquela casa? porque era mais fácil? estava isolada?, não tinha medidas de segurança?.

Nestes aspetos, era fácil ao nível da tecnologia ajudá-los, e já saberiam que determinados tipos de casas eram visadas pelo crime, possibilitaria um estudo e deste modo poder-se-ia canalizar os recursos para uma determinada zona de forma a impedir que isso voltasse a acontecer.

Para se atingir esse nível é necessário a sensibilidade de quem ande no patrulhamento a preencher esses campos, pois muitas vezes quem anda na rua não tem tempo, por vezes tem de passar tudo a papel e de seguida enviar um e-mail para enviar um formulário.

Possuir um meio tecnológico para logo de imediato, quando estiver a tomar conta da situação de uma forma simples, só a nível de toques e enviar, torna-se tudo mais rápido, por outro lado quem recebe essa informação, consegue pegar em toda essa informação e limitar e dar informação on-job, por exemplo aos sábados à noite a partir desta zona costuma haver muitos assaltos, isto seria uma forma de canalizar recursos e ao mesmo tempo prever o que viria a acontecer para se poder antecipar ao crime.

4. Quais os principais contributos da IA para o processamento de imagens a utilizar na segurança pública?

Para já na segurança pública, pessoas que estão desaparecidas, com a aplicação do reconhecimento facial para pessoas que são procuradas, se existissem câmaras seria mais fácil.

Ao nível da IA, porque a IA trata de forma mais rápida em comparação com a nossa visão, na segurança pública em zonas em que acontece algum crime, nós por algumas características desse sujeito, poderíamos encontrar mais facilmente o suspeito, porque imagine se está na baixa e houvesse uma confusão que derivou num esfaqueamento, ao recolher as características do suspeito e colocar numa imagem robô e se em seguida usar para pesquisar em fontes abertas como Facebook, isto possibilitaria determinar as possíveis pessoas compatíveis com o retrato robô.

Isto diminuiria o leque e seria mais fácil depois investigar desta lista quem esteve naquele local e aquela hora e seria mais fácil encontrar o suspeito.

Muitas vezes faz-se isto, eu vejo no reconhecimento facial a vantagem da IA neste aspeto, é a vantagem que possuímos com uma imagem procurar rapidamente e com a internet para procurar pessoas parecidas ou idênticas.

Outro aspeto, é em zonas de muita população, onde costuma haver muitos atropelamentos, com o reconhecimento facial seria mais fácil identificarmos qual seria a hora do dia onde passam mais carros.

Por exemplo em Inglaterra, têm implementado isso, as câmaras são uma ajuda para identificar suspeitos. Se possuir um software de IA ainda torna mais fácil a prevenção, para já, assim as pessoas estão mais alertas, pois estão a ser filmadas e qualquer ilícito criminal que eles façam vão ser responsabilizados, também ajuda em pequenos furtos que estão a acontecer e pela ação da filmagem conseguem contribuir para diminuir a incidência ou tentar minimizar esse aspeto, e pelo registo das câmaras, passado algum tempo conseguem recuperar o que foi furtado.

Vejo muitas vantagens na utilização de IA, o reconhecimento facial, a nível de imagens, e vai facilitar nos carros modernos, determinadas características que a IA vê, em aglomeração de pessoa junto a passadeira procede a redução automática da velocidade.

Se tivermos isso implementado quando houver um afluxo grande de pessoas na passadeira e o semáforo passar gradualmente de verde para laranja e depois vermelho, vai fazer com que a viatura que se aproxima em alta velocidade, comece logo a diminuir velocidade e por outro lado facilitar a passagem dos peões em segurança, isto seria uma ajuda na prevenção de acidentes rodoviários, de multas e outros, se houvesse já um sistema de IA neste sentido.

A IA pode ser um auxiliar para quem está no terreno, na atualidade por muito boa informação que se dê, os agentes por vezes estão envolvidos em tanta coisa ao nível legal, necessitam de saber de muitas leis e é muito difícil, a solução pode ser uma app, para tornar mais fácil e de forma simples, tratar a informação concisa, as pessoas não teriam de escrever muito, só teriam de selecionar, a recolha de dados para quem anda na rua, num formato de relatório de atualização periódica para acompanhar as mudanças da lei.

Permitir registar os contributos dos agentes num campo de questões relevantes, para futuramente poder ser avaliada a relevância desse dado para atualizar o relatório, automaticamente teríamos informação mais concisa e iríamos melhorando no dia a dia.

5. Gostaria de alertar ou de acrescentar algum comentário contributivo para o objetivo geral do trabalho?

Gostaria que a IA fosse um facilitador da atividade policial, por exemplo ao nível de pesquisa integrada como motor de busca, pode ser um auxiliar para identificar padrões.