



ACADEMIA MILITAR

Identificação de suspeitos: Sistemas de videovigilância na Guarda Nacional Republicana

Autor: Aspirante de Infantaria da GNR Ricardo Araújo de Almeida Mateus

Orientador: Major de Infantaria da GNR (Doutor) Tiago Miguel Gonçalves Silva

Coorientador: Major de Infantaria GNR Sara Isabel dos Santos Quinta Albuquerque

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Dissertação de Mestrado

Lisboa, 30 maio de 2023



ACADEMIA MILITAR

Identificação de suspeitos: Sistemas de videovigilância na Guarda Nacional Republicana

Autor: Aspirante de Infantaria da GNR Ricardo Araújo de Almeida Mateus

Orientador: Major de Infantaria da GNR (Doutor) Tiago Silva

Coorientador: Major de Infantaria GNR Sara Isabel dos Santos Quinta Albuquerque

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Dissertação de Mestrado

Lisboa, 30 maio de 2023

EPÍGRAFE

“Mudam-se os tempos, mudam-se as vontades,
Muda-se o ser, muda-se a confiança:
Todo o mundo é composto de mudança,
Tomando sempre novas qualidades.”
(Luís Vaz de Camões)

DEDICATÓRIA

À minha família e, em particular aos meus pais.

AGRADECIMENTOS

Este Relatório Científico Final do Trabalho de Investigação Aplicada representa o encerramento do Curso de Formação de Oficiais da Guarda Nacional Republicana, realizado na Academia Militar. É o resultado de uma etapa concluída, na qual enfrentamos várias dificuldades, contando com o apoio fundamental daqueles que estão próximos de nós.

Agradeço ao meu orientador, o Major de Infantaria da GNR (Doutor) Tiago Silva, pelo apoio constante, pelos conhecimentos transmitidos e pelo tempo dedicado à minha assistência ao longo desta pesquisa.

À Major Sara Albuquerque, minha coorientadora, agradeço pelos conhecimentos partilhados, pela disponibilidade durante todo o processo de investigação, pelos conselhos e por me desafiar a sempre melhorar o trabalho.

Agradeço a todos os militares que compartilharam seus conhecimentos, demonstrando sempre espírito de camaradagem e disponibilidade para me auxiliar durante todo o processo de elaboração da investigação.

Aos meus pais, agradeço por todo o apoio ao longo desta jornada na Academia Militar.

Aos meus colegas de curso, agradeço pela união e espírito de camaradagem vivenciados nos últimos cinco anos.

A todos vocês, expresso meu sincero agradecimento!

RESUMO

Ao longo das últimas décadas, os sistemas de videovigilância têm sido cada vez mais utilizados pelas polícias devido às suas potencialidades na prevenção, repressão e investigação criminal, entre outras. A videovigilância constitui um assunto fraturante da opinião da sociedade, gerando igualmente ideias discordantes entre diferentes autores. Atualmente, com a previsão e a divulgação da instalação de novos sistemas de videovigilância em Portugal, este tema ganhou uma nova projeção e mediatismo.

A investigação foi dividida numa parte teórica e numa parte prática. Na parte teórica foi efetuada uma revisão de literatura, onde é explanada o enquadramento legal relativo à utilização e recolha de imagens e à proteção de dados pessoais, quer no âmbito internacional quer nacional. É ainda feita referência a alguns conceitos, como é o caso dos CCTVs, aprofundando aquilo que são as suas vantagens e desvantagens.

Na parte prática foi adotado um método dedutivo com uma abordagem qualitativa, sendo feita a análise de inquéritos por entrevistas. A recolha de dados fez-se tendo em conta as técnicas de análise documental e realização de inquéritos por entrevista, as quais foram dirigidas à realidade da Guarda Nacional Republicana, ao Laboratório de Pesquisa Criminal e a forças congéneres europeias.

Em suma, da análise efetuada, incluindo nesta a análise documental, foi possível verificar que a Guarda Nacional Republicana, estando enquadrada no ordenamento jurídico português, tem tido alguma dificuldade em usar os sistemas de videovigilância em matéria de identificação de suspeitos devido às restrições impostas por lei e à qualidade das imagens que são recolhidas. No entanto, os sistemas de videovigilância e as imagens recolhidas nos mesmos são instrumentos proveitosos para a formulação de uma convicção criminal por parte do investigador.

Palavras-chave: CCTV, Videovigilância, Identificação de suspeitos, Investigação criminal, Prevenção criminal.

ABSTRACT

Over the past few decades, video surveillance systems have been increasingly used by the police due to their potential in crime prevention, repression, and investigation, among other purposes. Video surveillance is a divisive topic in society, generating conflicting ideas among different authors. Currently, with the announcement and dissemination of the installation of new video surveillance systems in Portugal, this subject has gained new prominence and media attention.

The research was divided into a theoretical part and a practical part. In the theoretical part, a literature review was conducted, which explains the legal framework regarding the use and collection of images and the protection of personal data, both internationally and nationally. Reference is also made to some concepts, such as CCTVs, delving into their advantages and disadvantages.

In the practical part, a deductive method with a qualitative approach was adopted, and the analysis was based on survey interviews. Data collection was carried out using techniques of document analysis and survey interviews, which were directed towards the reality of the Guarda Nacional Republicana, the Criminal Research Laboratory, and European counterpart forces.

In summary, based on the analysis conducted, including documentary analysis, it was possible to verify that the Guarda Nacional Republicana, being within the Portuguese legal framework, has faced some difficulties in using video surveillance systems for suspect identification due to legal restrictions and the quality of the images that are collected. However, despite these limitations, video surveillance systems and the images obtained from them are valuable tools for formulating a criminal conviction by investigators.

Keywords: CCTV, Video surveillance, Suspect identification, Criminal investigation, Crime prevention.

ÍNDICE GERAL

EPÍGRAFE	i
DEDICATÓRIA	ii
AGRADECIMENTOS	iii
RESUMO.....	iv
ABSTRACT	v
ÍNDICE GERAL	vi
ÍNDICE DE FIGURAS	viii
ÍNDICE DE TABELAS	ix
LISTA DE APÊNDICES E ANEXOS	x
LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS	xi
INTRODUÇÃO	1
PARTE I – ENQUADRAMENTO TEÓRICO	4
CAPÍTULO 1 – ENQUADRAMENTO LEGAL	4
1.1. Direito Internacional.....	4
1.2. Direito da União Europeia.....	5
1.3. Direito Nacional	7
CAPÍTULO 2 – VIDEOVIGILÂNCIA	11
2.1. Conceito CCTV	11
2.2. Valências	12
2.2.1. Videovigilância na Prevenção Criminal.....	13
2.2.2. Videovigilância na Investigação Criminal	14
2.3. Vantagens e Desvantagens	14
CAPÍTULO 3 – RECONHECIMENTO DE PESSOAS	22
3.1. Análise legal	22
3.2. Reconhecimento facial	23
3.2.1. Reconhecimento facial irrestrito: Maratona de Boston.....	27

PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO	33
CAPÍTULO 4 – DA METODOLOGIA, MÉTODOS E MATERIAIS	33
4.1. Natureza da investigação	33
4.2. Modelo de análise	33
4.3. Procedimento científico e metodológico	34
4.4. Amostragem: Composição e caracterização	35
4.5. Inquérito por entrevista	36
4.6. Métodos de recolha de dados	36
4.6.1. Tratamento e análise de dados	37
CAPÍTULO 5 – DA APRESENTAÇÃO E ANÁLISE DE RESULTADOS	38
5.1. Apresentação, análise e discussão dos inquéritos por entrevista	38
5.1.1. Apresentação, análise e discussão da questão nº1	38
5.1.2. Apresentação, análise e discussão da questão nº2	39
5.1.3. Apresentação, análise e discussão da questão nº3	40
5.1.4. Apresentação, análise e discussão da questão nº4	42
5.1.5. Apresentação, análise e discussão da questão nº5	43
5.1.6. Apresentação, análise e discussão da questão nº6	45
5.2. Análise comparativa a forças congéneres	46
CONCLUSÕES E RECOMENDAÇÕES	49
REFERÊNCIAS BIBLIOGRÁFICAS	52
APÊNDICES	I
Apêndice A – Inquérito por entrevista 1	II
Apêndice B – Inquérito por entrevista 2	VII
Apêndice C – Resposta ao inquérito por entrevista 1 – Entrevistado 1	XIII
Apêndice D – Resposta ao inquérito por entrevista 1 – Entrevistado 2	XVIII

ÍNDICE DE FIGURAS

Figura 1:Modelo 3D de um rosto feito a partir de duas imagens	26
Figura 2: Imagens faciais divulgados pelo FBI dos dois suspeitos dos atentados da Maratona de Boston.....	28
Figura 3: As três principais recuperações em uma pesquisa cega com o Neo Face 3.1.....	29
Figura 4:As três principais recuperações em uma pesquisa cega com o Face VACS 8.6...	29
Figura 5:As três principais recuperações em uma pesquisa cega com PittPatt 5.2.2	30
Figura 6:As três principais recuperações em uma pesquisa filtrada demograficamente com o NeoFace 3.1.....	31
Figura 7: As três principais recuperações em uma pesquisa filtrada demograficamente com o FaceVACS 8.6.....	31
Figura 8: As três principais recuperações em uma pesquisa filtrada demograficamente com PittPatt	32

ÍNDICE DE TABELAS

Tabela 1: Identificação dos entrevistados.....	36
Tabela 2: Apresentação e análise à questão 1.....	39
Tabela 3: Apresentação e análise à questão 2.....	40
Tabela 4: Apresentação e análise à questão 3.....	42
Tabela 5: Apresentação e análise à questão 4.....	43
Tabela 6: Apresentação e análise à questão 5.....	44
Tabela 7: Apresentação e análise à questão 6.....	46

LISTA DE APÊNDICES E ANEXOS

APÊNDICES Erro! Marcador não definido.

Apêndice A – Inquérito por entrevista 1..... **Erro! Marcador não definido.**

Apêndice B – Inquérito por entrevista 2..... **Erro! Marcador não definido.**

Apêndice C – Resposta ao inquérito por entrevista 1 – Entrevistado 1**Erro! Marcador não definido.**

Apêndice D – Resposta ao inquérito por entrevista 1 – Entrevistado 2**Erro! Marcador não definido.**

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

APA- Automated Teller Machine

CCTV- Circuito Fechado de Televisão

CEDH- Convenção Europeia para a Proteção dos Direitos Humanos

CNPD- Comissão Nacional de Proteção de Dados

CO- Comando Operacional

CPP- Código de Processo Penal

CPUI- Camaras Portáteis de Utilização Individual

CRP- Constituição da Republica Portuguesa

DIC- Direção de Investigação Criminal

DUDH- Declaração Universal dos Direitos Humanos

EER- taxa de erro de verificação

FAR- taxa de aceitação falsa

FBI- Federal Bureau of Investigation

FRR- taxa de rejeição falsa

GNR- Guarda Nacional Republicana

IC- Investigação Criminal

LPC- Laboratório de Polícia Científica

LPD- Lei de Proteção de Dados

MP- Ministério Público

OE- Objetivo Especifico

OPC- Órgão de Polícia Criminal

PSP- Polícia de Segurança Publica

QC- Questão Central

QD- Questão derivada

RGPD- Regulamento Geral de Proteção de Dados

TIA- Trabalho de Investigação Aplicada

UE- União Europeia

VSS- Video Surveillance System

INTRODUÇÃO

O presente Relatório Científico Final do Trabalho de Investigação Aplicada (TIA) é uma parte integrante do programa de mestrado em Ciências Militares, especialidade de Segurança da Guarda Nacional Republicana (GNR) da Academia Militar. O objetivo desta investigação é aplicar os conhecimentos adquiridos ao longo da formação na Academia Militar para obter o grau de mestre.

O tema abordado nesta pesquisa é "Identificação de Suspeitos: sistemas de videovigilância na Guarda Nacional Republicana".

O objetivo geral (OG) da investigação é perceber de que forma a utilização imagens e vídeos de sistemas de vídeo vigilância na GNR é uma mais valia em matéria de identificação de suspeitos de crimes. Assim defino dois objetivos específicos (OE): (OE1) perceber quais são as restrições no âmbito legal para a utilização de sistemas de vigilância; (OE2) avaliar, em termos de estudos comparativos, o que é que Portugal está a desenvolver em comparação com os nossos congéneres Europeus.

A presente investigação faz parte da etapa final do Curso de Formação de Oficiais e visa fornecer contribuições para o estudo de assuntos relevantes para a GNR. A investigação incide sobre o impacto que os sistemas de videovigilância têm em matéria de identificação de suspeitos e na redução da criminalidade após a sua implementação. Pretendendo por isso, perceber as capacidades que a GNR tem na sequência do acima descrito.

É amplamente reconhecido que estamos a avançar para um mundo cada vez mais tecnológico, no qual a ciência está a progredir rapidamente e trazendo consigo novos materiais. Neste contexto, acreditamos que é responsabilidade da GNR adaptar-se a essa nova tecnologia e aproveitá-la em benefício da segurança dos cidadãos.

Também estamos cientes de que a pequena criminalidade está a gerar um crescente sentimento de insegurança na sociedade em geral. Portanto, é imperativo que direcionemos a nossa atenção para esses tipos de problemas e priorizemos a prevenção, incutindo nas pessoas um senso de segurança sólido.

A criminalidade é um fenómeno extremamente complexo que se instala na sociedade e provoca um mal-estar generalizado. Não existe uma fórmula capaz de a fazer desaparecer, no entanto, existem formas de a prevenir, reduzindo assim drasticamente os seus números.

Em Portugal, nos últimos tempos, o Governo da República tem estado a promover com maior ênfase o uso da tecnologia de videovigilância. Acredita-se que a utilização da videovigilância desempenha um papel crucial no reforço das condições necessárias para a proteção de pessoas e propriedades, bem como na prevenção de atos criminosos. Além disso, a videovigilância proporciona uma maior eficácia operacional às Forças de Segurança em caso de incidentes e é considerada uma importante ferramenta complementar às suas atividades.

De acordo com Vieira (2011), o uso da videovigilância deve ser considerado como um complemento às ações das forças policiais, que são responsáveis pela prevenção e intervenção direta em incidentes. A videovigilância não deve ser encarada como uma alternativa devido à falta de recursos humanos.

A Comissão Nacional de Proteção de Dados (CNPd) reconhece que, em determinadas circunstâncias, a videovigilância pode ser necessária como um meio complementar de prevenção e apoio à investigação criminal (IC). Esse reconhecimento baseia-se nas características específicas da área sob vigilância, como ruas estreitas, cantos, esquinas e espaços de difícil visibilidade e controlo, nos quais a polícia de proximidade, mesmo em maior número, não conseguiria efetivamente monitorar e controlar.

Porém, prende-se aqui uma grande questão, que é levantada sempre que se fala da videovigilância em locais de domínio público de utilização comum, podendo mesmo se afirmar que é inerente a este: *os Direitos Fundamentais*.

Em relação à estruturação da investigação, esta foi ramificada em três capítulos, interligados entre si e com um desenrolar lógico ao longo do trabalho. No primeiro capítulo, onde é feita a abordagem conceptual, começamos por apresentar um enquadramento legal relativo ao tema da presente investigação, abordando de seguida um enquadramento teórico relativo aos sistemas de videovigilância fazendo referencia a alguns conceitos e às suas vantagens e desvantagens.

No segundo capítulo fazemos o enquadramento metodológico, onde apresentamos o modelo de análise e os objetivos da investigação, a estratégia e o método de abordagem, o desenho de pesquisa, as técnicas de recolha de dados, a amostragem tida em consideração, e a forma como foram analisados os dados.

No que diz respeito ao último capítulo, foi feita a apresentação, análise e discussão dos resultados, de onde consta o conteúdo das entrevistas realizadas aos dois grupos de entrevistados escolhidos, com utilidade para as conclusões e recomendações, parte final que representa o culminar de todo o trabalho desenvolvido até ao momento.

Este TIA teve a sua composição baseada na NEP 522/1^a – Normas para Redação de Trabalhos de Investigação, de 20 de janeiro de 2016, e em consonância com as normas American Psychological Association (APA), 7^a Edição, no que diz respeito às referências bibliográficas.

PARTE I – ENQUADRAMENTO TEÓRICO

CAPÍTULO 1 – ENQUADRAMENTO LEGAL

1.1. Direito Internacional

O tema em análise diz respeito à viabilidade de se implantar sistemas de vigilância, independentemente de ser em um espaço público ou não. No entanto, é importante salientar que tal medida acarreta limitações aos direitos, liberdades e garantias fundamentais dos cidadãos, tal como previsto na Constituição da Republica Portuguesa (CRP). Diante disso, os alcances e limites das restrições devem ser criteriosamente regulados por meio de legislação específica. Ademais, apesar da maioria das leis aplicáveis ser de caráter nacional, é imprescindível fazer menção a certos diplomas de natureza internacional e comunitária, cuja aplicação direta ou indireta tem tido uma significativa influência na elaboração de leis ordinárias sobre este tema.

De acordo com o disposto no artigo 8º da CRP, as normas e princípios de direito internacional geral ou comum, as normas presentes em convenções internacionais devidamente ratificadas ou aprovadas, bem como as normas emitidas pelos órgãos competentes das organizações internacionais das quais Portugal faz parte, desde que estejam previstas nos respectivos tratados constitutivos, são integrantes do direito português.

Nessa perspectiva, é necessário destacar a relevância da Declaração Universal dos Direitos Humanos (DUDH), a qual estabelece, no artigo 12º, a proteção contra intromissões arbitrárias na vida privada, família, domicílio ou correspondência, bem como a preservação da honra e reputação de qualquer indivíduo. De forma semelhante, o Pacto Internacional sobre Direitos Civis e Políticos prevê, em seu artigo 17º, que ninguém pode ser objeto de ingerências ilegais ou arbitrárias na sua vida privada, familiar, no seu domicílio ou correspondência, bem como ser alvo de ataques à honra e reputação.

Segundo Pereira (2019), embora esses documentos internacionais não abordem diretamente o tema da videovigilância, é importante ressaltar a possibilidade de imagens captadas poderem ser usadas para identificar uma pessoa, sendo consideradas como um dado pessoal, o que tem influenciado as leis ordinárias relacionadas com videovigilância.

1.2. Direito da União Europeia

No que diz respeito a documentos legais emitidos pela União Europeia (UE) que sejam relevantes para o estudo em questão, é importante mencionar diversos diplomas legais. A Convenção Europeia para a Proteção dos Direitos Humanos (CEDH), cujo artigo 8º estabelece que “qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.”, a Carta dos Direitos Fundamentais da UE, que de acordo com o artigo 7º, determina que “todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações”. Ainda no mesmo diploma, no artigo 8º estabelece que, “todos têm direito à proteção dos dados de carácter pessoal que lhes digam respeito sendo que esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei”.

No tocante ao Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, que veio revogar a Diretiva 95/46/CE (Regulamento Geral de Proteção de Dados (RGPD)) da qual foi aprovada a Lei nº 67/98 de 26 de outubro, (Lei de Proteção de Dados (LPD)), que surge na sequência da reforma de crescimento de 2012, e da Agenda Digital para a Europa, no seu artigo 1.º, determina que constituem objetivos da União Europeia: assegurar “a proteção das liberdades e dos direitos fundamentais das pessoas singulares, nomeadamente do direito à vida privada, no que diz respeito ao tratamento de dados pessoais” e aplica-se “ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos num ficheiro ou a ele destinados”. Devendo entender-se por dados pessoais, de acordo com o seu artigo 4º, “qualquer informação relativa a uma pessoa singular identificada ou identificável”. Contudo, a identificação pode resultar de forma direta ou indireta, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social. Segundo o artigo 5º do mesmo regulamento, determina-se que os dados devem ser submetidos a um tratamento que observe a licitude e a legalidade. É imprescindível que sejam coletados para finalidades específicas, explícitas e legítimas, sem excessos em relação às intenções estabelecidas para sua obtenção e posterior processamento. Adicionalmente, devem ser precisos e, se necessário, atualizados, bem como armazenados de modo que permita a identificação das partes interessadas apenas durante o tempo

essencial à consecução dos fins objetivados por sua coleta e processamento subsequente. No que diz respeito aos critérios para o tratamento legítimo desses dados, a norma requer o consentimento claro e inequívoco da pessoa em causa, portanto, é necessário que essa pessoa conceda sua permissão de forma inequívoca. Esse consentimento não será exigido quando estiverem preenchidas algumas das outras alíneas do artigo 6º do regulamento, mais concretamente, nos termos da alínea f), “o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.” O regulamento estabelece nos seus artigos 13º e 14º que, ao submeter uma pessoa ao tratamento de dados, o responsável pelo tratamento deve fornecer-lhe informações essenciais para garantir a integridade do tratamento dos dados. Isso inclui a identificação do responsável pelo tratamento, as finalidades do tratamento dos dados, informações sobre destinatários, a natureza obrigatória ou facultativa da resposta, bem como possíveis consequências em caso de não resposta, a disponibilidade do direito de acesso e correção dos dados relacionados à pessoa em questão. Nos termos do artigo 82º do mesmo diploma legal, “qualquer pessoa que tenha sofrido danos materiais ou imateriais devido a uma violação do presente regulamento tem direito a receber uma indemnização do responsável pelo tratamento ou do subcontratante pelos danos sofrido”. Verificamos assim, que o Regulamento (UE) 2016/679, segundo Pereira (2019), traz consigo um aumento da confiança do consumidor nas novas transações comerciais e digitais, através de várias medidas: a promoção da capacidade de controle dos dados pessoais pelo próprio consumidor, o reforço dos direitos dos titulares dos dados pessoais, o reforço da segurança dos dados em resposta ao risco cibernético e a exigência de uma atitude responsável e proativa por parte das organizações que utilizam dados pessoais, a fim de garantir a privacidade e segurança desses dados. Tudo isso contribui para uma maior confiança dos consumidores nas transações digitais e comerciais.

Comparando assim a Diretiva 95/46/CE com o novo RGPD, este mantém um processo de continuidade na aplicação dos conceitos de “dados pessoais”, “tratamento”, “consentimento”, “responsável pelo tratamento e entidade subcontratante”, “autoridade de controlo”, entre outros. No entanto, traz consigo novas figuras jurídicas, como a “pseudonimização e anonimização”, proteção de dados desde a conceção e por defeito, violação da segurança dos dados pessoais, consulta prévia, avaliação de impacto, registo das atividades de tratamento, encarregado de proteção de dados e a consagração de outros direitos do titular dos dados. De acordo com Pereira (2019), na sequência do novo

RGPD, foi elaborada a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativa à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.

1.3. Direito Nacional

O tema da utilização da informática é abordado de forma geral na nossa Constituição de 1976, dedicando apenas o artigo 35º à temática da videovigilância. Neste artigo, o nº 2 determina que a lei deve definir o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, garantindo a sua proteção por meio da CNPD.

Dado o carácter sensível da questão, a regulamentação da videovigilância e dos dados pessoais foi deixada para a legislação ordinária, através da referência do artigo 35º da CRP. Como resultado, surgiram vários diplomas que regulamentam este tema no nosso país: A Lei n.º 95/2021, de 29 de dezembro, que veio regular a utilização pelas forças e serviços de segurança, de sistemas de videovigilância, dando relevância no seu artigo 14º para a utilização de sistemas de videovigilância de qualquer entidade pública ou privada, instalados em locais públicos ou privados de acesso ao público nos casos previstos no artigo 3º. Ainda no mesmo artigo é possível verificar que no que toca a matéria de identificação de suspeitos as forças e serviços de segurança podem visualizar as imagens recolhidas pelos sistemas referidos anteriormente, para efeitos de identificação de autor de ilícito criminal, se houver suspeitas que o autor ainda se encontra no local. É importante ainda realçar, que no seu artigo 15º, para os fins previstos nas alíneas c), e), f) e k) do n.º 1 do artigo 3º, as forças e serviços de segurança podem, mediante autorização prévia do dirigente máximo, captar imagens, com recurso a câmaras fixas ou portáteis, exclusivamente para efeitos de visualização, sem gravação, sendo possível proceder à respetiva gravação em caso de deteção de factos com relevância criminal; A Lei n.º 34/2013, de 16 de maio, que veio estabelecer o regime do exercício da atividade de segurança privada e proceder à primeira alteração à Lei n.º 49/2008, de 2 de agosto regulando também a utilização dos meios de videovigilância no âmbito da segurança privada e dos serviços de autoproteção explanados no seu artigo 31º que de acordo com o mesmo, as entidades titulares de alvará ou de licença para o exercício dos serviços previstos nas alíneas a), c) e d) do n.º 1 do artigo 3.º de mesmo diploma legal podem utilizar sistemas de vigilância por câmaras de vídeo para captação e gravação de imagem com o

objetivo de proteger pessoas e bens, desde que sejam ressalvados os direitos e interesses constitucionalmente protegidos, sendo obrigatório o seu registo na Direção Nacional da Polícia de Segurança Pública (PSP), nos termos definidos por portaria do membro do Governo responsável pela área da administração interna. A Portaria n.º 273/2013, de 20 de agosto veio regular e definir as condições específicas da prestação dos serviços de segurança privada previstos no artigo 3º da Lei n.º 34/2013, de 16 de maio. Esta determina, nomeadamente, os requisitos mínimos das instalações e meios materiais e humanos das entidades de segurança privada previstos no artigo 3º da Lei n.º 34/2013, de 16 de maio; os requisitos técnicos mínimos dos sistemas e medidas de segurança aplicáveis às instituições de crédito e às sociedades financeiras previstos no artigo 8º da Lei n.º 34/2013, de 16 de maio; os requisitos técnicos mínimos dos sistemas e medidas de segurança aplicáveis às entidades gestoras de conjuntos comerciais e de grandes superfícies de comércio previstos no artigo 8º da Lei n.º 34/2013, de 16 de maio; os requisitos técnicos mínimos dos sistemas e medidas de segurança aplicáveis aos estabelecimentos onde se proceda à exibição, compra e venda de metais preciosos e obras de arte, bem como a farmácias e postos de abastecimento de combustível previstos no artigo 8º da Lei n.º 34/2013, de 16 de maio; Os requisitos técnicos dos equipamentos, condições de funcionamento e modelo de comunicação dos alarmes previstos no artigo 11º da Lei n.º 34/2013, de 16 de maio; Os procedimentos de registo dos sistemas de videovigilância e os avisos legais e simbologia identificativa previstos no artigo 31º da Lei n.º 34/2013, de 16 de maio; O Decreto-Lei n.º 207/2005, datado de 29 de novembro, estabeleceu a regulamentação dos meios de vigilância eletrónica rodoviária utilizados pelas forças de segurança. Este documento estabeleceu os procedimentos a serem seguidos pelas forças de segurança ao instalar sistemas de vigilância eletrónica rodoviária. Além disso, o decreto definiu as formas e condições em que esses sistemas poderiam ser usados pelas forças de segurança, seja instalado pela Estradas de Portugal ou por empresas concessionárias rodoviárias em suas respetivas vias concessionadas. O documento também definiu os procedimentos a serem seguidos para o tratamento da informação coletada e o registo eficaz de acidentes, infrações ou quaisquer ilícitos. Por fim, o decreto estabeleceu as formas através das quais as forças de segurança se coordenariam com as empresas legalmente autorizadas a utilizar os equipamentos de vigilância rodoviária para garantir uma interação eficaz. Contudo, é de salientar que em termos práticos não existe uma estratégia a nível nacional uma vez que as instalações destes sistemas não se encontram devidamente e uniformemente colocados havendo, portanto, zonas com relevância criminal que poderiam ser sujeitas à instalação de sistemas de vídeo

vigilância, mas que as mesmas não se encontram pois em Portugal é executada uma estratégia a nível local deixando a decisão da instalação para as concessionárias rodoviárias e para os municípios; A Lei n.º 51/2006, de 29 de agosto, que veio regular a instalação e utilização de sistemas de vigilância eletrónica rodoviária e a criação, utilização de sistemas de informação de acidentes e incidentes pela EP — Estradas de Portugal, e pelas concessionárias rodoviárias; A Lei n.º 33/2007, de 13 de agosto, veio regular o serviço de videovigilância em táxis, fixando as finalidades autorizadas, os requisitos mínimos, as características dos equipamentos e o regime aplicável à sua homologação, instalação e fiscalização; A Lei n.º 58/2019, de 08 de Agosto, que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que veio revogar a Diretiva 95/46/CE (RGPD); Mais recentemente, e que é de extrema relevância abordar temos o Decreto-Lei n.º 2/2023, de 2 de janeiro de 2023, que define as normas de colocação, ativação, sinalização e utilização das câmaras portáteis de uso individual (CPUI), assim como a forma de transmissão, armazenamento e acesso aos dados recolhidos e as características e requisitos técnicos mínimos das CPUI, podendo estas ser usadas para gravação da prática de ilícitos criminais entre outras situações explanadas no seu artigo 7º, como também Decreto-Lei n.º 87/2021, de 20 de outubro de 2021, que de acordo com o seu artigo 18º estabelece normas de operação para atividades isentas (serviços aduaneiros, de busca e salvamento, de vigilância, prevenção e combate a incêndios ou em atividades e serviços similares, sob o controlo, responsabilidade e no interesse do Estado) e o regime sancionatório aplicável às aeronaves não tripuladas, bem como determina os termos de definição das áreas geográficas.

Tendo em conta a temática em análise da presente investigação, surge também a importância de realçar aquilo que é a visão do legislador em relação ao uso de sistemas de videovigilância fazendo uma comparação destes com as escutas. Neste sentido é possível verificar que em termos de garantia da privacidade do cidadão o legislador prevê um maior controlo naquilo em que se traduz as escutas do que na recolha e tratamento de imagem e som na via pública. Ao analisar esta comparação de uma forma mais detalhada podemos verificar que, por exemplo a nível de autorização, enquanto que de acordo com a Lei n.º 95/2021, de 29 de dezembro, no seu artigo 15º as forças e serviços de segurança apenas necessitam de uma autorização prévia do dirigente máximo para captar imagens, com recurso a câmaras fixas ou portáteis, exclusivamente para efeitos de visualização, sem gravação, sendo possível proceder à respetiva gravação em caso de deteção de factos com

relevância criminal, no Código de Processo Penal (CPP) no seu artigo 187º podemos verificar um elevado número de condições a que está sujeito o pedido de autorização para as forças de segurança efetuarem escutas sendo que este terá ainda de ser dirigido por despacho fundamentado ao juiz de instrução e mediante requerimento do Ministério Público (MP).

Considerando o expressivo número de diplomas legais aprovados para a transposição da Diretiva 95/46/CE e as disposições do RGPD, é possível inferir que o tratamento de dados pessoais é um tema extremamente sensível e complexo. Tal complexidade se deve à natureza delicada e problemática desse assunto, uma vez que envolve direitos pessoais e impõe restrições significativas aos direitos fundamentais, à liberdade e à reserva da intimidade da vida privada dos cidadãos.

Em razão desse cenário, de acordo com Pereira (2019), torna-se imprescindível que tanto o legislador ordinário quanto o internacional estejam constantemente preocupados em estabelecer de que maneira e por quem os dados pessoais devem ser tratados, assim como determinar os princípios orientadores que norteiam essa temática, a fim de minimizar quaisquer dúvidas e promover a efetiva proteção dos direitos fundamentais dos cidadãos. No entanto, subsistem ainda “incertezas” relativamente, até onde poderão ser restringidos os direitos fundamentais, acima identificados, em nome da prevenção e da garantia do direito da segurança nacional, valores igualmente constitucionais e fundamentais.

CAPÍTULO 2 – VIDEOVIGILÂNCIA

2.1. Conceito CCTV

Os sistemas de videovigilância, também conhecidos como circuitos fechados de televisão (CCTV), têm-se tornado cada vez mais presentes em nosso cotidiano. Contudo, a definição desses sistemas não é clara na literatura, uma vez que muitos autores assumem que é um conceito amplamente conhecido. Portanto, é crucial explorar esse conceito a fim de garantir que não haja ambiguidade no seu uso (Goold, 2004).

Os sistemas de CCTV são uma tecnologia multifuncional que pode ser encontrada em diversas áreas de atividade diária. Seu uso principal está relacionado à gestão de riscos em situações como congestionamentos de tráfego, incêndios, acidentes e crimes. No entanto, devido ao potencial de controle social que esses sistemas podem gerar, alimentando visões distópicas, eles podem ser caracterizados como "tecnologia de risco", pois são criados para enfrentar os riscos, mas também representam um risco em si mesmo (Hempel & Töpfer, 2002).

Estes sistemas podem também ser descritos como um sistema em que várias câmaras estão ligadas em circuito fechado ou loop, no qual as imagens geradas são enviadas para um monitor central de televisão ou gravadas para visualização posterior. Originalmente, o termo foi concebido para distinguir esses sistemas privados dos demais canais de televisão - nos quais qualquer recetor devidamente ajustado pode capturar as imagens enviadas pelas câmaras - e, desde então, refere-se a praticamente qualquer tipo de sistema de vigilância que utiliza câmaras de vídeo. Atualmente, esses sistemas são amplamente utilizados em diversas atividades diárias, como o controle de tráfego, monitorização de estradas, coleta de informações sobre clientes por grandes cadeias de supermercados, observação do trabalho de cirurgiões em salas de cirurgia hospitalares, monitorização do controle de produção em linhas de montagem de fábricas, entre outros. No entanto, embora sejam empregados em uma ampla variedade de locais, a maioria dos sistemas comerciais disponíveis é utilizada para fins de segurança (Goold, 2004).

Os sistemas de videovigilância são compostos por uma ligação comunicativa entre as câmaras de vigilância e os monitores de controle. Este complexo sistema é controlado e manipulado por um operador central encarregado do posicionamento das câmaras e das imagens visualizadas nos monitores (Vieira, 2011).

Segundo Ratcliffe (2006), podemos distinguir dois tipos de sistemas de videovigilância, com base na participação humana: o sistema passivo, no qual existe um dispositivo de gravação das imagens, podendo estas ser repetidas posteriormente caso ocorra um crime, mas sem que ninguém monitorize ativamente as imagens; e o sistema ativo, no qual uma pessoa monitoriza em tempo real uma série de ecrãs com imagens em tempo real. Contudo, na prática, muitos sistemas são híbridos, com dispositivos de gravação a registar todas as imagens e um operador a observar cada monitor, concentrando-se em alguns e ignorando outros.

Através da implementação dos sistemas de videovigilância, estrategicamente posicionados para permitir a monitorização exaustiva de um determinado espaço, com a captação minuciosa de todos os movimentos realizados, é possível criar um efeito de onipresença (Vieira, 2011). Nesse sentido, Frois (2013), encara estes sistemas como um mecanismo de poder baseado na capacidade de disciplinar e controlar as pessoas através da sua exposição a uma entidade invisível e desconhecida, que, por si só, induz mudanças de comportamento sem a necessidade de uma interação direta.

A localização desses sistemas é normalmente determinada após consulta às autoridades locais, polícia e fornecedores, e, de acordo com o propósito do sistema, são colocados de forma a fornecer a maior cobertura possível de vigilância. Em geral, o local de instalação é definido com base nos padrões criminais, de modo que o sistema possa abranger as áreas de maior incidência de crimes (McLean, Worden e Kim, 2013).

Em resumo, o conceito de CCTV consiste na vigilância de indivíduos e espaços físicos por meio de câmaras instaladas em áreas específicas. As imagens captadas pelas câmaras podem ser visualizadas em tempo real em monitores e também podem ser gravadas. Para aumentar a segurança, muitos desses sistemas são monitorados e controlados por um operador.

2.2. Valências

Os sistemas de videovigilância, quando instalados em espaços públicos de uso comum, desempenham um papel crucial na prevenção e repressão de crimes e comportamentos antissociais. Eles são uma ferramenta valiosa e complementar às atividades policiais, permitindo uma resposta rápida e eficaz a situações de emergência. Além disso, esses sistemas têm um forte efeito dissuasor sobre aqueles que poderiam estar a pensar em cometer crimes ou em ter comportamentos inapropriados em áreas públicas (Sousa, 2009).

A utilização de sistemas de videovigilância permite às autoridades identificar e responsabilizar criminosos, tornando as comunidades mais seguras e aumentando a confiança do público nas forças de segurança. A capacidade desses sistemas em ajudar a polícia a cumprir várias funções policiais, tais como informações, prevenção, repressão e assistência, torna-os altamente versáteis e valiosos (Alves, 1996, p.5).

Com o uso de tecnologia de vigilância, é possível melhorar significativamente a eficácia da aplicação da lei em áreas públicas. Ao fornecer evidências tangíveis, os sistemas de videovigilância podem ajudar a resolver casos de crime mais rapidamente e de forma mais eficaz. Ao mesmo tempo, os sistemas também ajudam a prevenir a ocorrência de crimes, reduzindo a incidência de comportamentos antissociais e aumentando o sentimento de segurança entre as populações abrangidas pelo sistema.

Em resumo, os sistemas de videovigilância em áreas públicas de uso comum são uma ferramenta valiosa e multifacetada para as forças de segurança, permitindo uma resposta rápida e eficaz a situações de emergência e ajudando a prevenir e reprimir crimes e comportamentos antissociais. Eles são altamente versáteis e podem ser usados em várias funções policiais, contribuindo para melhorar a segurança e a confiança do público nas autoridades.

2.2.1. Videovigilância na Prevenção Criminal

A implementação da videovigilância em locais públicos tem como uma de suas principais razões a necessidade de prevenir e reprimir crimes. Como Goold (2004, p.3) afirma, a videovigilância é uma "nova e valiosa arma na luta contra o crime e a desordem pública". A simples presença das câmaras já possui um grande efeito dissuasor, contudo é importante que os possíveis criminosos estejam cientes da presença das câmaras e de que acreditem que há um risco significativo de deteção e detenção caso realizem algum crime, para que abdicuem de suas intenções criminosas (Ratcliffe, 2006).

O estudo desenvolvido pela consultora PremiValor para a ADT, intitulado "Segurança, Proteção de Dados e Privacidade em Portugal", obteve resultados interessantes. De acordo com o estudo, 73% dos participantes consideram que os meios de videovigilância são dissuasores de comportamentos ilícitos. Este dado reforça a importância da videovigilância como um meio de prevenção criminal, além de destacar a sua eficácia em dissuadir indivíduos de cometerem crimes.

Em resumo, a videovigilância em locais públicos é vista como uma valiosa ferramenta na prevenção e repressão de crimes e comportamentos ilícitos. A presença das

câmaras é altamente dissuasora, especialmente se os criminosos estiverem cientes de sua existência e dos riscos envolvidos em cometer um crime na presença de tais dispositivos. Além disso, o estudo da PremiValor para a ADT reforça a eficácia da videovigilância como um meio dissuasor de comportamentos ilícitos, enfatizando sua importância na prevenção criminal.

2.2.2. Videovigilância na Investigação Criminal

Além das vantagens no âmbito da prevenção criminal, o sistema de CCTV representa uma ferramenta valiosa para as forças policiais no que diz respeito à investigação de atividades criminosas (Uribe, 2006). A capacidade de gravação contínua proporcionada por esta tecnologia permite que as autoridades utilizem as imagens gravadas para identificar suspeitos e esclarecer incidentes.

Outro benefício significativo da videovigilância na IC é a possibilidade de utilizar as imagens capturadas pelas câmaras de vigilância como prova em tribunal. Em Portugal, de acordo com os artigos 164º a 167º do CPP, é permitido o valor probatório das reproduções mecânicas, o que pode aumentar a possibilidade de condenação dos criminosos quando cientes de que suas ações foram registradas (Madaleno, 2007).

2.3. Vantagens e Desvantagens

Tornou-se cada vez mais comum a presença de sistemas de videovigilância (CCTV) em espaços públicos, os quais se configuram como uma das principais estratégias utilizadas em todo o mundo para prevenir crimes, especialmente os que afetam pessoas e património. Contudo, é importante destacar que o elevado custo de instalação e manutenção desses sistemas é uma desvantagem evidente (Frois, 2013).

Ao utilizar o CCTV como técnica de prevenção situacional, procura-se aumentar a vigilância com o objetivo de aumentar os riscos associados à prática de crimes, levando potenciais criminosos a desistir de suas intenções ao perceberem o risco de serem identificados e capturados (Ratcliffe, 2006). No entanto, mesmo diante da presença de câmaras de segurança, existem pessoas que continuam a cometer crimes, seja por falta de conhecimento da presença do sistema, falta de preocupação em ser identificado ou por utilização de substâncias psicotrópicas ou álcool que afetam seu julgamento (Short & Ditton, 1998).

Para que os sistemas de vigilância possam ser efetivos como elemento dissuasor, é preciso que a população esteja ciente de sua presença e entenda que o risco de detecção e captura aumenta com a existência do CCTV (Ratcliffe, 2006). Além disso, é importante lembrar que a utilização de CCTV também pode reduzir o sentimento de insegurança, fornecer suporte à IC, coletar informações e fornecer outros benefícios (Welsh & Farrington, 2009).

Uma das desvantagens apontadas para o uso do sistema de vigilância por CCTV é a possível transferência do crime para outras áreas geográficas, onde os criminosos possam continuar a cometer crimes sem restrições (Repetto, 1976). Embora aumente o custo de cometer um crime em locais com câmaras de segurança, isso pode resultar numa transferência do crime para outras áreas, sem redução da criminalidade global (Fernandes, 2006). No entanto, Ratcliffe (2009) argumenta que, mesmo que haja uma transferência de crime para outras áreas, ainda há um ganho líquido na prevenção do crime. Ele observa que pode haver também uma mudança no *modus operandi* do crime, o que ele chama de deslocamento tático. Como exemplo, ele cita o tráfico de drogas em Londres, onde a presença de câmaras de segurança levou a uma mudança no método de entrega, passando a ser feito por telemóvel, que era um método pouco eficaz na época, resultando numa diminuição do tráfico e, conseqüentemente, do crime.

No entanto, embora seja possível que ocorra transferência da criminalidade para outras áreas, esse fenômeno não é inevitável. De acordo com Hesseling (1994), que analisou 55 estudos sobre medidas de prevenção criminal, a transferência da criminalidade é possível, mas não é generalizada. O autor argumenta que mesmo quando ocorre, esse fenômeno é limitado tanto em termos de dimensão quanto de alcance. Isso ocorre porque há limites para a capacidade de adaptação do delinquente. À medida que se torna mais difícil e arriscado cometer um crime, o delinquente terá cada vez menos opções e, muitas vezes, essas opções exigirão um grande esforço adaptativo para encontrar alternativas viáveis, o que pode levar à desistência completa da prática do crime em questão.

Por outro lado, a instalação de sistemas de vigilância por CCTV pode levar ao fenômeno da difusão de benefícios, o que significa que os benefícios resultantes da sua utilização também podem ter efeitos em áreas adjacentes (Clarke & Weisburd, 1994). Por exemplo, os criminosos podem não ter conhecimento preciso do alcance das câmaras e, portanto, sentir-se vigiados numa área mais ampla do que a realmente coberta pelo sistema CCTV, reduzindo a criminalidade nesses locais (Clarke & Weisburd, 1994). Além disso, as medidas de prevenção situacional, ao atacarem um problema específico, podem ter efeitos

sobre outros tipos de crime que ocorrem na mesma área. O uso de sistemas de CCTV pode ser visto como um esforço das autoridades para melhorar a segurança pública, e isso pode reforçar o controle social informal, aumentando a consciência cívica das pessoas e incentivando a sua participação ativa na prevenção da criminalidade (Ratcliffe, 2006). Por outro lado, ao sentir-se mais segura, a população tende a utilizar mais o espaço público, o que aumenta a vigilância natural (McLean, Worden, & Kim, 2013). De acordo com Smith, Clarke e Pease (2002), a cobertura mediática em torno da instalação de sistemas de CCTV pode antecipar os benefícios desses sistemas, uma vez que a dinâmica criada em torno da instalação pode aumentar o risco percebido pelos infratores potenciais.

Segundo a perspectiva de Valente (2012), existem desvantagens inerentes associadas ao sistema de videovigilância, como o perigo de se avançar para uma gradual "robotização da sociedade", devido à falta de emotividade associada ao uso desses meios. Este meio pode representar uma "submissão do homem à máquina" que, se não for cuidadosamente gerida, pode resultar na "deterioração da riqueza humana: o pensamento" (Valente, 2012). Além disso, o autor acrescenta que o sistema de videovigilância pode reduzir a componente humana presente no contato direto entre a polícia e o cidadão, uma vez que, com a ativação da videovigilância, pode surgir uma tendência para reduzir o número de agentes policiais presentes na área monitorada. No entanto, é possível refutar esta questão com base no argumento apresentado por Ratcliffe (2006), que defende que o aumento da vigilância pode levar a uma maior identificação de crimes (que anteriormente passavam despercebidos), o que pode evidenciar a necessidade de aumentar o efetivo policial em determinadas áreas.

Uma das principais vantagens da instalação de sistemas de vigilância por câmaras em espaços públicos é a sua capacidade de diminuir o sentimento de insegurança da população, independentemente de ser real ou apenas percebido. Embora o medo do crime possa não estar correlacionado com a taxa de criminalidade, o que importa para a maioria das pessoas é sentir-se protegida (Frois, 2011). Esse sentimento de insegurança pode ser composto por duas dimensões distintas: uma objetiva, relacionada com a criminalidade efetivamente cometida contra uma pessoa ou seus bens, e outra subjetiva, desenvolvida no plano psicológico, que produz sentimentos de medo pessoal e preocupações de segurança (Oliveira, 2006). Portanto, o medo do crime pode ser desproporcional ao crime real, assumindo proporções mais graves do que o próprio crime. A instalação de câmaras de vigilância em locais públicos pode contribuir para reduzir o nível de insegurança percebido, transmitindo a sensação de que todas as infrações serão gravadas e permitirão a intervenção policial (Moreira, 2013). No entanto, isso pode ter efeitos distintos nas pessoas, aumentando

o sentimento de segurança em algumas e transmitindo a sensação de que o local é inseguro para outras (Ratcliffe, 2006).

De acordo com Frois (2016), o sentimento de insegurança é complexo e subjetivo, variando de pessoa para pessoa. É difícil medir esse sentimento, já que os inquéritos de vitimização mostram que o grau de subjetividade é muito grande. Frois (2016) considera que as câmaras de vigilância podem ser úteis na redução do sentimento de insegurança. No entanto, isso também pode levar a um falso sentimento de segurança, fazendo com que as pessoas confiem excessivamente no sistema de vigilância e desconsiderem as medidas de autoproteção que antes praticavam, aumentando assim a probabilidade de serem vítimas de crime (Ladeira, 2006).

Em termos de IC, as câmaras de vigilância são uma vantagem, pois as imagens podem ajudar na identificação de suspeitos e seu *modus operandi*, na identificação de testemunhas (Ratcliffe, 2006) e são fundamentais na produção de prova indispensável à resolução de investigações (Ashby, 2017). De acordo com Piza, Caplan e Kennedy (2014), os crimes detetados e reportados pelo sistema de vigilância apresentam taxas de arquivamento menores do que os crimes reportados através do número de emergência, uma vez que as infrações detetadas através do sistema de vigilância certamente estarão gravadas. Além disso, a utilização das imagens como prova pode aumentar a confissão de suspeitos (Ladeira, 2006).

No entanto, é importante ter cuidado na seleção das imagens que serão usadas como prova, pois certas imagens podem levar os suspeitos a perceber o alcance e o funcionamento das câmaras, levando a uma alteração do *modus operandi* ou deslocalização do crime. Ainda na IC, mesmo que o CCTV não permita visualizar o ato criminoso, poderá revelar pormenores fundamentais para a investigação. Em Portugal, no dia 20 de maio de 2017, na Damaia, cerca de uma semana após o início de funcionamento do CCTV da Amadora, um taxista foi assassinado na sequência de um assalto num local não abrangido pelo CCTV, no entanto, as imagens captadas pelas câmaras próximas do local, apesar de não captarem o momento do homicídio, permitiram a identificação dos suspeitos e serviram de prova no processo criminal que terminou com a condenação do homicida a pena de prisão.

Por fim, compreende-se que a videovigilância no espaço público pode acarretar uma desvantagem significativa, uma vez que, embora o seu propósito seja garantir o direito fundamental à segurança, pode implicar restrições a outros direitos, liberdades e garantias, tais como o direito à imagem, à liberdade de movimentos e à reserva da vida privada (Guerra, et al., 2004). No entanto, segundo a CRP, o Artigo 27º consagra tanto o direito à liberdade

quanto o direito à segurança, reconhecendo que estes direitos estão intimamente relacionados desde as primeiras constituições liberais (Canotilho & Moreira, 1993).

Conforme os estudos de Canotilho e Moreira (1993), o direito à liberdade não implica uma liberdade geral, mas sim as principais liberdades em que esta se concretiza, incluindo, como subdireito, o direito à proteção do Estado contra os atentados de outrem à própria liberdade. Por sua vez, o direito à segurança tem como significado essencial a garantia de exercício seguro e tranquilo dos direitos, livre de ameaças ou agressões.

Embora seja uma das missões da Polícia a prevenção de crimes, a garantia da segurança e, conseqüentemente, da liberdade das pessoas, tal deve ser feito com respeito pelos direitos, liberdades e garantias dos cidadãos (Artigo 272º n.º 3 da CRP), uma vez que, como apontado por Dias (1998), o Estado, suas instituições, seus órgãos e seus agentes estão todos subordinados à Constituição e à Lei, e não é aceitável que qualquer poder e autoridade sejam exercidos de forma ilimitada, irracional, desproporcionada ou incontrolável.

Portanto, a Lei n.º 95/2021, de 29 de dezembro, numa tentativa de equilibrar as possibilidades e desvantagens dos sistemas de videovigilância, restringe a instalação de câmaras de vigilância para fins muito específicos, somente quando estas forem o meio mais adequado para o efeito, e a utilização de câmaras de vídeo deve ser regida pelo princípio da proporcionalidade, ou seja, deve haver uma ponderação caso a caso, tendo sempre em conta a possibilidade e o grau de afetação dos direitos pessoais.

É ainda importante realçar que segundo Gill et al, (2005), após a realização de um estudo que permitiu averiguar as principais mudanças na criminalidade depois da instalação de catorze sistemas de CCTV em Inglaterra avaliados como parte de uma Avaliação Nacional de CCTV descrevendo as nuances por trás de cada sistema. Cada sistema de CCTV definiu seus próprios objetivos, embora todos os sistemas avaliados tivessem dois objetivos gerais: reduzir o crime e o medo do crime.

De acordo com o estudo realizado quarenta e sete câmaras foram adicionadas a um sistema existente no centro da cidade de Londres, estendendo-o para áreas residenciais e industriais adjacentes e conectando-o a um sistema hospitalar. Após a sua instalação, o crime registado diminuiu 28% e esta diminuição foi estatisticamente maior do que o controlo, sugerindo que o CCTV pode ter contribuído para a redução do crime nesta área. Os crimes diminuíram, enquanto os delitos mais espontâneos apresentaram um aumento. A preocupação em ser vítima de um crime também diminuiu. Vários fatores de confusão ocorreram durante o período de avaliação, o que poderia explicar parcialmente a diminuição do crime e a preocupação com o mesmo. Foram ainda instaladas seiscentas e quarenta e seis

câmaras em 60 estacionamentos de transporte público de Londres, 58 das quais foram avaliadas. O crime com veículos teve uma redução estatisticamente significativa de 73% após a instalação das câmaras. Os parques de estacionamento experimentaram diferentes níveis de criminalidade e aqueles com um nível alto e médio de risco de crime sofreram reduções estatisticamente significativas de 80% e 62%, enquanto os parques de estacionamento de baixo risco apresentaram uma diminuição não estatisticamente significativa de 37%. A queda acentuada no crime demonstrou um efeito dissuasor. A polícia também recebeu provas que lhes permitiram prender criminosos conhecidos, mostrando que o sistema também funcionava para identificação de suspeitos da prática de crimes. Todos os estacionamentos tiveram um alto nível de cobertura (todos, exceto dois, atingiram 100% de cobertura) e a maioria era independente, com entradas e saídas cobertas por câmaras.

Contudo, apenas as duas situações acima referidas foram bem sucedidas e mostraram mudanças significativas na redução da criminalidade, o que leva os autores a concluir que o impacto do CCTV tem sido variável. Por outro lado, foram realçadas as várias questões que afetam o funcionamento do CCTV. Em suma, é importante lembrar que as características das áreas e os problemas de criminalidade nelas gerados variam consideravelmente, e a adequação do CCTV dependerá, no mínimo, da natureza desses problemas, da presença de outras medidas, do compromisso e das habilidades da administração e da equipa para fazer o CCTV funcionar. A crença de que o CCTV por si só pode combater problemas sociais complexos é irrealista ao extremo. Na melhor das hipóteses, o CCTV pode funcionar junto com outras medidas para gerar algumas mudanças, mas não é uma solução milagrosa sendo que ainda há muito a ser aprendido sobre como o usar da melhor maneira possível.

Analisando ainda um relatório elaborado por Brandon e Farrington (2002) podemos observar que o presente estudo apresenta uma revisão sistemática dos efeitos do CCTV no crime e segue de perto a metodologia desta técnica de revisão. As revisões sistemáticas usam métodos rigorosos para localizar, avaliar e sintetizar evidências de estudos de avaliação anteriores e são relatadas com o mesmo nível de detalhe que caracteriza os relatórios de pesquisa original de alta qualidade. De acordo com Johnson e cols. (2000, p. 35), as revisões sistemáticas “abordam essencialmente de forma epidemiológica as seções de metodologia e resultados de uma população específica de estudos para chegar a um consenso baseado em pesquisas sobre um determinado tópico de estudo”. Estas têm objetivos e critérios explícitos para incluir ou excluir estudos, pesquisas extensas para estudos de avaliação elegíveis de todo o mundo, extração e codificação cuidadosa das suas principais características e um relatório estruturado e detalhado dos métodos e conclusões da revisão.

Uma série de pesquisas direcionadas e abrangentes da literatura publicada e não publicada e contatos com pesquisadores importantes produziram 22 avaliações de CCTV que atenderam aos critérios de inclusão desta revisão, os critérios de inclusão exigiam programas de CCTV que empregassem projetos de avaliação rigorosos para avaliar os efeitos sobre o crime, com o projeto mínimo envolvendo medidas antes e depois do crime em áreas de controle experimentais e comparáveis.

Foram incluídas 22 avaliações realizadas em três ambientes principais: centros urbanos e habitações públicas, transportes públicos e estacionamentos. As avaliações não foram distribuídas uniformemente entre as três configurações. O maior número de avaliações ocorreu no centro da cidade/habitação pública. Das 22 avaliações incluídas, metade (11) encontrou um efeito desejável sobre o crime e cinco encontraram um efeito indesejável sobre o mesmo. Cinco avaliações encontraram um efeito nulo sobre o crime (ou seja, evidência clara de nenhum efeito), enquanto a outra foi classificada com um efeito incerto sobre o crime (ou seja, evidência pouco clara de efeitos). Os resultados de uma meta-análise fornecem uma imagem mais clara da eficácia do CCTV na prevenção do crime. A partir de 18 avaliações – as outras quatro não forneceram os dados necessários para serem incluídas na meta-análise – concluiu-se que o CCTV teve um efeito desejável significativo sobre o crime, embora a redução geral do crime tenha sido de apenas quatro por cento. Metade dos estudos (nove em 18) mostraram evidências de um efeito desejável do CCTV no crime sendo os mesmos realizados Reino Unido. Por outro lado, os outros nove estudos não mostraram qualquer efeito desejável do CCTV no crime. Todos os cinco estudos norte americanos estavam nesse grupo.

A meta-análise também examinou o efeito do CCTV na tipologia de crimes mais frequentes, onde se pode constatar que o CCTV não teve efeito sobre crimes violentos (cinco estudos), mas teve um efeito desejável significativo sobre crimes com veículos envolvidos (oito estudos).

Nos três ambientes em estudo onde se fez sentir uma maior evidência dos efeitos do CCTV foi nos estacionamentos, verificou-se uma redução estatisticamente significativa no crime, cerca de 41% em áreas experimentais em comparação com áreas de controle. No entanto, para todos os estudos neste cenário, outras medidas estavam em operação ao mesmo tempo que o CCTV.

Por fim, com este estudo os autores concluíram que o CCTV reduz o crime em pequeno grau. À luz dos resultados bem-sucedidos, os futuros esquemas de CCTV devem

ser cuidadosamente implementados em diferentes configurações e devem utilizar processos de avaliação de alta qualidade com longos períodos de acompanhamento.

Como podemos perceber, existem várias vantagens e desvantagens associadas à utilização de sistemas de videovigilância. Atualmente, não há uma resposta única e definitiva para a questão crucial de saber se a videovigilância é eficaz ou não. De acordo com o European Forum for Urban Security (2010), as respostas para todas essas questões devem ser avaliadas de acordo com o contexto em que as câmaras estão a ser usadas. Em outras palavras, cada cidade deve ser analisada individualmente, levando em consideração fatores específicos, como tamanho do território e número de câmaras, entre outros.

CAPÍTULO 3 – RECONHECIMENTO DE PESSOAS

3.1. Análise legal

Na versão atual do artigo 147.º do Código de Processo Penal (CPP), intitulado "Reconhecimento de Pessoas", o legislador sentiu a necessidade de estabelecer os procedimentos que devem ser seguidos no reconhecimento de pessoas. Isso ocorre porque o reconhecimento de uma pessoa é influenciado pelas circunstâncias em que essa prova é produzida, sendo necessário estabelecer regras mínimas para garantir a confiabilidade das informações obtidas.

Segundo Carvalho (2013), torna-se por isso relevante focar alguns aspetos de natureza genérica relevantes para a análise deste meio de prova: a lei não estabelece qualquer restrição sobre as pessoas que podem fazer um reconhecimento (testemunhas, assistentes, demandantes, coarguidos); a competência para determinar a realização de reconhecimentos pertence ao Ministério Público, ao Juiz de Instrução ou ao Juiz de Julgamento (conforme a fase processual em que o mesmo for determinado); o juízo de necessidade sobre a realização de um reconhecimento cabe à entidade que preside à fase processual em que o mesmo ocorre.

Analisando mais pormenorizadamente, o número um do presente artigo estabelece a necessidade de regulamentar os procedimentos relacionados ao reconhecimento de pessoas, pois o reconhecimento de uma pessoa é influenciado pelas circunstâncias em que essa prova é realizada. O objetivo é estabelecer regras mínimas que visam garantir a validade das informações obtidas. No referido artigo, são estipulados formalismos obrigatórios, ou seja, um conjunto de questões que devem ser seguidas. Inicia-se com a descrição da pessoa a ser identificada pela testemunha, exigindo que todos os detalhes de que se lembra sejam indicados. No entanto, de acordo com Merca (2021), parte-se do pressuposto de que a recuperação da memória é algo fácil para o ser humano, o que não corresponde à realidade, como será explicado posteriormente. Em seguida, a norma aborda se a pessoa já foi vista anteriormente e em que condições, finalizando com a questão sobre a existência de circunstâncias que possam afetar a credibilidade da identificação.

No seu número dois, estabelece-se que, quando a identificação não é conclusiva, presume-se que, ao contrário, quando é conclusiva, o procedimento formal de reconhecimento é encerrado. Caso a identificação não seja conclusiva, a norma determina que a pessoa encarregada do reconhecimento deve afastar-se e chamar, pelo menos, duas pessoas que se assemelhem o máximo possível à pessoa a ser identificada. Destaca-se a

necessidade de que o vestuário seja semelhante ao da pessoa a ser identificada, e exige-se que a pessoa a ser identificada seja colocada numa linha de reconhecimento ao lado das demais pessoas, idealmente nas mesmas condições em que foi vista pela testemunha. Nesse momento, a testemunha é chamada e questionada se reconhece alguma das pessoas que compõem a linha de reconhecimento e, em caso afirmativo, qual é a pessoa reconhecida.

Dado o tema da atual investigação, é de extrema relevância elaborar uma análise ao número cinco do presente artigo, em que o mesmo estabelece, de forma obrigatória, que, caso haja um reconhecimento por fotografia, filme ou gravação, este só terá valor probatório se for seguido por um reconhecimento presencial, de acordo com o número dois do artigo 147.º do Código de Processo Penal. Nesta situação, o legislador português não teve em consideração a influência que o primeiro reconhecimento, através de fotografia, poderá ter nos reconhecimentos subsequentes.

No artigo, é estabelecido no número sete que, caso o ato de reconhecimento não cumpra integralmente as normas estabelecidas, ele não terá valor como meio de prova em qualquer fase do processo.

Dentro desse contexto, o Código de Processo Penal, no seu artigo 147º, apresenta um instrumento regulador para a obtenção da prova, destacando sua natureza autónoma como meio de prova, não sendo considerado apenas um subtipo da prova testemunhal. Esse instrumento consiste na reconstituição das percepções visuais ocorridas anteriormente, limitando-se à evocação de percepções olfativas ou auditivas, sem proibi-las. Trata-se de um ato de carácter inquisitório, no qual ocorre a confrontação visual de alguém apontado como autor de um ilícito, invocando a capacidade de recorrer à memória (Gama et al, 2021, p. 337).

3.2. Reconhecimento facial

O reconhecimento facial é uma técnica biométrica que se baseia nos traços do rosto humano. Esse processo de reconhecimento é realizado através da medição de pontos faciais, que estabelecem uma conexão algorítmica entre características e tamanhos, como, por exemplo, a distância precisa entre o nariz e as orelhas, o tamanho do crânio, a arcada dentária, entre outros detalhes (Okabe & Carro 2014).

O problema do reconhecimento automático de faces é uma tarefa complexa que envolve a deteção e localização de faces num ambiente confuso, seguida de normalização e reconhecimento. Houve algumas pesquisas neste âmbito que exploraram como os seres humanos realmente reconhecem os indivíduos. Neste sentido Bruce et al. (1999) realizaram

um estudo de modo a compreender como é que as pessoas reconhecem outras e descobriram, através de experiências, que em imagens de baixa qualidade, a combinação de informações da cabeça, corpo e vestuário desempenha um papel importante nesse reconhecimento.

Segundo Bramble et al. (2001), é evidente a presença de vários sistemas comerciais de reconhecimento facial (como o FaceIt, Mandrake, Marlin, entre outros) sendo comercializados em todo o mundo. Esses sistemas são baseados em diversas abordagens matemáticas, tais como Análise de Componentes Principais (Eigenfaces), comparação de características dos componentes e Redes Neurais Feedforward. Muitos desses sistemas e técnicas foram testados utilizando o banco de dados FERET (Face Recognition Technology) e alcançaram taxas de sucesso de 96% ou mais.

Com base numa análise dessas técnicas, Grudin (2000) afirma que é impossível para qualquer abordagem única atualmente disponível alcançar uma precisão de 100% devido à complexidade do rosto. Além disso, o mesmo faz referência à impossibilidade de selecionar o melhor método de reconhecimento facial e que por essa razão, provavelmente, esses sistemas têm aplicação limitada na aplicação da lei e na ciência forense.

Por outro lado, segundo Phillips et al. (2003), a comparação e o reconhecimento facial automatizado ainda não estão a funcionar de forma ideal. Os sistemas de maior qualidade apresentam uma taxa de erro de verificação (EER) de aproximadamente 5%, uma taxa de rejeição falsa (FRR) de cerca de 10% e uma taxa de aceitação falsa (FAR) de 1%, quando são utilizadas imagens de "qualidade de documento" em condições de iluminação controlada. Os sistemas de reconhecimento facial ainda são sensíveis ao envelhecimento dos indivíduos: o FRR aumenta para cerca de 20% a uma taxa de FRR de 1% se a imagem tiver 3 anos de idade.

No que diz respeito ao desempenho dos sistemas de biometria facial para fins de investigação de criminosos ou terroristas numa lista de observação (identificação), os melhores sistemas conseguem identificar aproximadamente 60% dos suspeitos numa lista de 1000 pessoas num determinado ambiente, resultando em 1% de alarmes falsos.

É importante salientar que estes resultados são baseados em experiências com imagens padronizadas de alta a média qualidade, utilizando indivíduos colaboradores. O desempenho dos sistemas biométricos de reconhecimento facial diminui significativamente quando ocorrem alterações na pose, posição, iluminação e expressão facial. Testes realizados com um sistema automatizado de bom desempenho (em experiências próprias) resultaram numa EER de 1,5% ao utilizar apenas imagens frontais. No entanto, essa taxa aumentou para 11% ao utilizar apenas imagens em ângulo de $\frac{3}{4}$, seja à esquerda ou à direita, e subiu para

24% ao combinar imagens frontais e em ângulo de $\frac{3}{4}$. Imagens capturadas por câmaras de vigilância em ambientes não controlados, com qualidade padrão e colocadas maioritariamente em locais visíveis (como no alto de tetos ou em caixas multibanco), e que gravam pessoas que não estão a olhar diretamente para a câmara, com expressões variáveis e rostos por vezes parcialmente cobertos, são de difícil reconhecimento pelos sistemas biométricos (FIDIS, 2009).

No entanto, existem alguns projetos piloto nos quais modelos 3D são comparados com fotografias 2D. O Laboratório Forense da Holanda analisou o posicionamento de uma pessoa ou crânio para a comparação de fotos, utilizando análises de três pontos e uma fotografia 3D (Heuve, 1998). Eles adquiriram as imagens 3D através de um sistema desenvolvido no projeto IMPROOFS, que é agora comercializado pela Eyetronics. Segundo Yoshino et al. (2000), outro projeto do National Research Institute of Police Scene, no Japão, analisou a comparação de fotos 3D com 2D. O modelo 3D é alinhado na mesma posição da imagem 2D. A distância e o ângulo entre os pontos de seleção pré-definidos nas imagens 2D e 3D são medidos automaticamente, e é feita uma comparação com base na diferença ponto a ponto entre ambas as imagens.

A confiabilidade da reconstrução do tecido facial no crânio tem sido questionada devido à incerteza na relação entre o osso e os tecidos moles do rosto. De acordo com Michael (1999), a ausência de dados científicos reconhecidos levou a debates, controvérsias e ceticismo em relação à reconstrução facial no passado, o que resultou na falta de aceitação generalizada pela comunidade forense. No entanto, nos últimos anos, com a existência de recursos computacionais mais poderosos, combinada com um aumento significativo de dados científicos, levou ao surgimento da visualização e análise de dados volumétricos como uma importante aplicação da computação gráfica. A visualização e interpretação eficientes e precisas desses dados, como a renderização volumétrica, estão atualmente em investigação por parte dos meios de comunicação e instituições científicas.



Figura 1: Modelo 3D de um rosto feito a partir de duas imagens

Fonte: software package “D me know”

Segundo Bramble et al. (2001), os sistemas de reconhecimento facial podem ser configurados para corresponder um para um (verificação ou autenticação) ou um para muitos (identificação). Em ambos os processos, duas faces são comparadas e um valor correspondente é determinado. No modo de verificação, um nível de confiança é estabelecido e, se o valor de correspondência exceder esse limite, a correspondência é considerada bem-sucedida e a identidade é verificada. Na comparação um para muitos, os sistemas calculam o grau de semelhança entre o rosto capturado e aqueles associados aos indivíduos conhecidos armazenados no banco de dados de imagens faciais. Em seguida, é gerada uma lista de possíveis indivíduos, classificados em ordem decrescente de pontuação. Com base nessa lista reduzida, um operador irá determinar se o indivíduo está presente ou não no banco de dados. A lista reduzida é utilizada com o objetivo de minimizar o tempo necessário para que o operador examine o banco de dados de rostos. Esse tipo de aplicação para sistemas de reconhecimento facial está sendo utilizado pelas autoridades como uma ferramenta de inteligência.

Segundo FIDIS (2009), no Instituto Forense da Holanda, atualmente, é prática realizar imagens de reconstrução com suspeitos, sempre que possível, para permitir comparação manual por especialistas. No entanto, a experiência tem mostrado que, em condições não controladas, com variações significativas de iluminação, fundos complexos e em movimento, oclusões parciais ou totais, as técnicas de detecção facial também apresentam um desempenho substancialmente reduzido. Isso tem um efeito significativo nos resultados do reconhecimento facial, uma vez que a saída da primeira etapa (detecção facial) é uma das principais entradas para a segunda etapa (reconhecimento facial). Por esse motivo, há um

esforço contínuo para melhorar as técnicas de extração de fundo e detecção facial, bem como para enriquecer a tarefa de reconhecimento com outras partes do corpo.

O sistema de reconhecimento facial na comparação forense enfrenta uma limitação importante, uma vez que não existe uma correlação conhecida entre os valores de correspondência e a probabilidade de uma comparação. Portanto, não é possível determinar se alguém tem um valor de correspondência superior ou quantas outras faces possuem valores de correspondência semelhantes. Este problema foi reconhecido por Phillips et al. (2003), que afirmou: "O reconhecimento facial num mundo com bilhões de pessoas é um desafio complexo, uma vez que os investigadores têm apenas alguns milhares de imagens de indivíduos e apenas um número reduzido de imagens para cada um deles".

3.2.1. Reconhecimento facial irrestrito: Maratona de Boston

Em 15 de abril de 2013, às 14h49, ocorreram duas explosões perto da linha de chegada da Maratona de Boston, resultando na morte de 3 pessoas e ferindo outras 264. Pouco depois do atentado, mais de 1.000 polícias de várias agências iniciaram uma investigação, recorrendo a fontes de informação, consultando bases de dados governamentais e públicas, e realizando entrevistas com testemunhas oculares. Foi solicitado às empresas que revisassem e preservassem as gravações de videovigilância, e a polícia recebeu uma "enorme quantidade de evidências em vídeo" por parte do público. Após analisar "fotos, vídeos e outras evidências", o Federal Bureau of Investigation (FBI) divulgou imagens e vídeos dos dois suspeitos mostrados na Figura 2. Além de procurar ajuda na identificação, a divulgação das imagens e vídeos também visava limitar o dano causado a pessoas erroneamente apontadas como suspeitas através de notícias e redes sociais. Logo após a divulgação, os dois suspeitos foram identificados como irmãos, Tamerlan Tsarnaev e Dzhokhar Tsarnaev, pela sua tia, que fez uma chamada para a linha de denúncias do FBI (Montgomery et al. 2013).



Figura 2: Imagens faciais divulgados pelo FBI dos dois suspeitos dos atentados da Maratona de Boston

Fonte: Relatório Técnico MSU-CSE-13-4

Foi então elaborado um estudo por Klontz e Jain (2013), através reconhecimento facial irrestrito, usando imagens de domínio público dos dois suspeitos nos atentados da Maratona de Boston. O reconhecimento irrestrito envolve a comparação de uma imagem de consulta capturada sem a cooperação do sujeito e geralmente apresenta maiores variações em fatores que podem causar confusão, como pose, iluminação, expressão, resolução e oclusão.

Foram conduzidos dois estudos distintos para avaliar o desempenho de três sistemas comerciais de reconhecimento facial de última geração (NeoFace 3.1, FaceVACS 8.6 e PittPatt 5.2.2) em diferentes cenários.

Na pesquisa cega, cada sonda é comparada com todas as imagens da galeria sem utilizar as informações demográficas (por exemplo, gênero, etnia e idade) associadas aos rostos das imagens.

As Figuras 3, 4 e 5 apresentam os três principais resultados de cada sonda para os sistemas NeoFace 3.1, FaceVACS 8.6 e PittPatt 5.2.2, respectivamente. É evidente que o uso de óculos de sol pelo irmão mais velho, Tamerlan Tsarnaev, prejudicou significativamente suas correspondências principais. Inconsistências gerais entre os dados demográficos de cada investigação e seus principais resultados da galeria sugerem que a filtragem demográfica poderia melhorar a precisão.

Sonda	Posição 1	Nível 2	Nível 3
			
			
			
			
			

Figura 3: As três principais recuperações em uma pesquisa cega com o Neo Face 3.1.

Fonte: Relatório Técnico MSU-CSE-13-4

Sonda	Posição 1	Nível 2	Nível 3
			
			
			
			
			

Figura 4:As três principais recuperações em uma pesquisa cega com o Face VACS 8.6.

Fonte: Relatório Técnico MSU-CSE-13-4



Figura 5:As três principais recuperações em uma pesquisa cega com PittPatt 5.2.2

Fonte: Relatório Técnico MSU-CSE-13-4

Na pesquisa filtrada, cada sonda é comparada apenas com imagens de uma galeria que possua dados demográficos semelhantes (Klare et al. 2012)

Para o Suspeito 1 (branco, sexo masculino, idade entre 20 e 30 anos) e Suspeito 2 (branco, sexo masculino, idade entre 15 e 25 anos), a aplicação do filtro reduziu a quantidade de imagens de referência de um milhão para 174.718 e 131.462 imagens, respectivamente.

As Figuras 6, 7 e 8 mostram os três principais retornos de cada sonda para NeoFace 3.1, FaceVACS 8.6 e PittPatt 5.2.2, respectivamente. A filtragem demográfica melhora substancialmente as classificações de recuperação em comparação com a pesquisa cega, com uma melhoria proporcional à redução da quantidade de imagens de referência.



Figura 6: As três principais recuperações em uma pesquisa filtrada demograficamente com o NeoFace 3.1.

Fonte: Relatório Técnico MSU-CSE-13-4



Figura 7: As três principais recuperações em uma pesquisa filtrada demograficamente com o FaceVACS 8.6.

Fonte: Relatório Técnico MSU-CSE-13-4



Figura 8: As três principais recuperações em uma pesquisa filtrada demograficamente com PittPatt

Fonte: Relatório Técnico MSU-CSE-13-4

Embora o caso dos atentados na Maratona de Boston ofereça apenas um pequeno número de imagens faciais disponíveis para correspondência automática, é possível retirar informações valiosas da interpretação dos resultados. Embora tanto o NeoFace como o FaceVACS demonstrem alta precisão no reconhecimento convencional de foto a foto, o algoritmo NeoFace apresenta um desempenho significativamente melhor nos testes de reconhecimento facial irrestrito.

No entanto, segundo Klontz e Jain (2013), mesmo com o NeoFace, a precisão da correspondência ainda não é suficientemente precisa para uma implementação "no escuro" em aplicações de aplicação da lei. É necessário fazer mais progressos na superação de desafios como pose, resolução e oclusão, de forma a aumentar a utilidade das imagens faciais em condições irrestritas. Ainda assim, com a utilização de filtragem demográfica, várias investigações e a intervenção humana no processo, os comparadores faciais de última geração têm o potencial de auxiliar na aplicação da lei na detenção de suspeitos de forma oportuna.

PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO DE CAMPO

CAPÍTULO 4 – DA METODOLOGIA, MÉTODOS E MATERIAIS

4.1. Natureza da investigação

Este estudo está a ser realizado no âmbito de um TIA, que é necessário para concluir a formação académica exigida para a obtenção do grau de mestre. Com base na revisão bibliográfica realizada, é possível compreender a perceção de alguns autores sobre a temática, a abordagem mais adequada para investigar a problemática e as questões que surgiram durante a investigação desses autores.

O objetivo desta pesquisa é compreender a importância do processo de aprendizagem, a fim de obter informações que permitam alcançar os objetivos desejados com método e rigor (Biblioteca do Instituto Superior Técnico, 2015, p.13). Este estudo aplicado tem uma abordagem prática e exploratória, visando aumentar o conhecimento sobre o tema. Além disso, é descritivo, apresentando uma explicação detalhada do assunto, e explicativo, buscando uma melhor compreensão da problemática e oferecendo respostas à questão central e às questões derivadas propostas para a pesquisa. Para garantir a observância desses aspetos ao longo da investigação, é necessário seguir "etapas organizadas de forma sistemática, em uma sequência específica", ou seja, "um conjunto de etapas que, quando executadas de maneira sistemática, facilitam a aquisição de conhecimentos" (Jung, 2009, p.37), ou seja, um método científico.

No próximo capítulo, será apresentada a metodologia utilizada nesta pesquisa. Serão abordados o modelo de análise, os procedimentos científicos e metodológicos, a amostragem e a coleta e tratamento dos dados.

4.2. Modelo de análise

Considerando que uma investigação científica é conduzida com o objetivo de encontrar respostas para um problema ou resolvê-lo, isto é, que ela é "um sistema de produção de conhecimento, com base em meios de trabalho determinados" (Romão, 2021, p.6), as perguntas formuladas para a pesquisa visam fornecer respostas aos problemas

existentes e resolvê-los. Assim, a questão central (QC) e consequentes questões derivadas (QD), são:

QC: “Qual a mais-valia para a identificação de suspeitos de crimes para a GNR da utilização de imagens e vídeos de sistemas de vídeo vigilância em Portugal?”

QD.1- “Haverá restrições no âmbito legal para a utilização de sistemas de vigilância?”

QD.2- “Em termos de estudos comparativos o que é que Portugal está a desenvolver, em comparação com os nossos congéneres Europeus?”

Com vista ao explanado nas perguntas para a presente investigação, importa perceber qual o papel que a captação de imagens e vídeos através de sistemas de vídeo vigilância tem em matéria de identificação de suspeitos na GNR desempenha e de que forma é que o ordenamento jurídico em Portugal influencia a utilização dos sistemas de vídeo vigilância. Por fim, realizar um estudo comparativo entre Portugal e os nossos congéneres Europeus a fim de perceber os desenvolvimentos que estão a ser efetuados nesta matéria.

4.3. Procedimento científico e metodológico

De acordo com Severino (2013, p.89), a ciência faz uso de um método próprio, o método científico, que é um elemento fundamental do processo de produção de conhecimento científico, o que a diferencia do senso comum. Isso significa que a ciência utiliza o método científico para produzir conhecimento científico, que é diferente do conhecimento adquirido pelo senso comum. Embora esse conhecimento científico não seja superior, é obtido por meio do método científico e está em constante evolução (Silva, M., Costa, E., Costa, A., 2013).

A presente pesquisa emprega uma abordagem qualitativa, utilizando entrevistas semiestruturadas com militares experientes no assunto em estudo. Essas entrevistas fornecem dados relevantes sobre o objeto de estudo, enquanto a análise documental também serve como fonte de conteúdo para a produção de conhecimento.

Em relação à estratégia de pesquisa adotada, foi escolhida uma abordagem qualitativa, na qual o pesquisador desempenha um papel fundamental para alcançar os objetivos. Nessa abordagem, a interpretação dos fenômenos sociais e a atribuição de significados são baseadas em padrões identificados nos dados, com o propósito de confirmar teorias ou verificar hipóteses (Vilelas, 2009, p. 105).

Uma vez definida a estratégia a adotar na presente investigação torna-se necessário abordar qual o desenho de pesquisa que melhor se adequa a este trabalho. Como tal, e uma vez que se pretende utilizar métodos de comparação através de entrevistas com outros países mais desenvolvidos nesta matéria com fim de perceber de que maneira é que a GNR poderá evoluir neste aspeto, optou-se pela utilização do desenho de pesquisa de estudo comparativo. Este tipo de desenho de pesquisa é empregue quando se deseja estudar dois ou mais casos contrastantes utilizando métodos semelhantes. A lógica subjacente à comparação baseia-se na ideia de que os fenómenos sociais são mais facilmente compreendidos quando são comparados com outros casos ou situações que apresentam diferenças significativas entre si (Bryman, 2012, p. 72).

Por fim, método utilizado para a investigação, é o método dedutivo, “um método que parte do geral e, a seguir, desce para o particular” (Prodanov & Freitas, 2013, p.27), ou seja, “parte de princípios reconhecidos como verdadeiros e indiscutíveis e possibilita chegar a conclusões de maneira puramente formal, isto é, em virtude unicamente da sua lógica” (Gil, 2008, p.9).

4.4. Amostragem: Composição e caracterização

Considerando que o tempo disponível para a investigação é limitado, torna-se necessário selecionar uma amostra representativa a partir de uma população mais ampla. Conforme apontado por Mello (2018), é essencial obter informações da população em estudo, e a amostragem desempenha um papel fundamental nesse processo de pesquisa. Para compreender as perspetivas e comportamentos da população em geral, é necessário selecionar uma amostra representativa de um grupo específico dentro do público-alvo. Conforme destacado por Jeová (2016), a amostragem é crucial nesse sentido.

Na escolha da amostra, levamos em consideração as funções desempenhadas pelos militares e especialistas entrevistados no contexto da identificação de suspeitos por meio de sistemas de videovigilância. Com base nos objetivos estabelecidos, optamos por uma amostragem não probabilística por conveniência, incluindo os participantes aos quais o pesquisador tem maior acesso.

4.5. Inquérito por entrevista

O público-alvo das entrevistas são militares da GNR e especialistas da polícia científica com experiência em matéria de investigação criminal e sistemas de videovigilância. Os entrevistados consistem, no diretor da Direção de Investigação Criminal (DIC) e de um especialista da polícia criminal do Laboratório de Polícia Científica (LPC).

Entrevistado	Unidade/ Subunidade	Função	Posto/Cargo	Habilitações Literárias	Data
E1	Direção de Investigação Criminal do Comando Operacional	Diretor da DIC	Tenente- Coronel	Mestre	05/05/2023
E2	Laboratório de Polícia Científica	Especialista de Polícia Científica	Especialista de Polícia Científica	Licenciado	10/05/2023

Tabela 1: Identificação dos entrevistados

Fonte: Elaboração Própria

4.6. Métodos de recolha de dados

O processo de recolha de informações é uma etapa crucial em qualquer pesquisa científica e deve ser planeado com cuidado e rigor. Segundo Sousa & Baptista (2011), este procedimento operacional deve ser claramente definido e executado de forma precisa, a fim de possibilitar a pesquisa e garantir sua qualidade. É crucial que a coleta de dados seja empírica, ou seja, baseada em observações e evidências concretas (Pardal & Lopes, 2011). É importante considerar que a natureza e os objetivos da pesquisa podem influenciar o processo de coleta de dados (Carvalho, 2015), e é necessário adaptar o procedimento para que seja adequado ao contexto específico da investigação.

Para o desenvolvimento da presente investigação, foram utilizadas técnicas de recolha de dados, nomeadamente a análise documental e o inquérito por entrevista. Estes métodos são complementares entre si e têm como objetivo fornecer informações relevantes para a investigação em questão (Alves, 2017). A análise documental permite complementar

as informações obtidas por outras técnicas, contribuindo assim para uma maior compreensão do objeto de estudo (Matos, 2015). Por sua vez, o inquérito por entrevista implica um contacto direto entre o investigador e os interlocutores, permitindo obter informações adaptadas às especificidades do objeto de estudo (Quivy & Campenhoudt, 1992). Conforme destacado por Borg e Gall (2002), uma das principais vantagens desse método de coleta de dados é a sua capacidade de se adaptar, permitindo assim obter o máximo de informações possível.

A opção pelo uso de metodologias qualitativas e pela combinação de técnicas de recolha de dados, visa compensar as limitações e pontos cegos de cada método, contribuindo para uma maior qualidade e rigor na investigação realizada (Brayman, 2012). É importante referir que a escolha dos métodos de recolha de dados deve ser planeada e organizada de forma rigorosa, a fim de garantir a qualidade e eficiência da investigação realizada (Sousa & Baptista, 2011).

Em suma, a utilização de múltiplas técnicas de recolha de dados na presente investigação tem como objetivo fornecer informações complementares e adaptadas ao objeto de estudo, permitindo uma análise mais completa e rigorosa da problemática em causa.

4.6.1. Tratamento e análise de dados

De acordo com Quivy e Campenhoudt (1992), é importante reconhecer que a realidade é mais complexa do que inicialmente concebida durante o processo de investigação. À medida que a informação é recolhida, é necessário analisar e interpretar os factos inesperados que surgem, o que pode exigir uma reavaliação das questões iniciais. Esse processo de reflexão e adaptação das questões é essencial para alcançar conclusões válidas e abrangentes.

Neste sentido, a análise documental realizada foi de extrema importância, pois as informações obtidas permitiram direcionar uma nova investigação com base em informação relevante sobre o tema em estudo, conforme referido por Bardin (1977).

Nesta fase da investigação, percebemos o enquadramento legal relativamente aos sistemas de vídeo vigilância e a recolha e tratamento de imagem e som. de seguida foi realizada um enquadramento teórico relativo à vídeo vigilância onde foram apresentados alguns conceitos e as suas vantagens e desvantagens. Assim, e após enquadrar todo o aspeto teórico, um estudo mais aprofundado do mesmo era essencial.

CAPÍTULO 5 – DA APRESENTAÇÃO E ANÁLISE DE RESULTADOS

5.1. Apresentação, análise e discussão dos inquéritos por entrevista

Com base nas informações fornecidas, pode-se inferir que neste subcapítulo do trabalho serão apresentados os resultados obtidos a partir dos inquéritos por entrevista realizados com o primeiro grupo de entrevistados. Esses resultados serão cuidadosamente analisados e discutidos, levando em consideração todo o conteúdo teórico abordado ao longo da investigação. Além disso, será realizada uma comparação entre os resultados obtidos e as informações obtidas por meio da análise documental realizada.

5.1.1. Apresentação, análise e discussão da questão nº1

A questão nº 1 **“Quais são os sinais característicos que permitem a identificação de um suspeito?”** tem como objetivo perceber quais são as características humanas que possibilitam a identificação de pessoas e reconhecimento de pessoas.

Relativo a esta questão o E1 enumerou várias características humanas passivas de serem identificativas do ser humano como por exemplo a lofoscopia, genética, através da face, da íris, da voz e da morfologia de algumas partes constituintes do corpo humano (por exemplo, a orelha) referindo-se a estas como características únicas de cada ser humano.

Diferentemente, o E2 apenas se cingiu a características possíveis de serem identificáveis através de imagens retiradas de sistemas de videovigilância, referindo que, dificilmente se poderá atingir uma identificação dada a reduzida qualidade das imagens e os detalhes específicos do rosto humano, contudo a mesma exigiria a realização de uma comparação facial com uma imagem controlada (amostra referência).

Questão nº1 Quais são os sinais característicos que permitem a identificação de um suspeito?	
Nº	Resposta
E1	“A lofoscopia (impressões datiloscópicas) e a genética (ADN) são duas disciplinas que permitem a identificação de uma pessoa com valor probatório absoluto.” “Existem outras características individuais que permitem reconhecer/identificar o ser humano, nomeadamente através da face, da retina, da íris, da voz, da morfologia de algumas partes constituintes do corpo humano, entre outras.” “O seu estudo tem por base critérios de similitude demonstrativa de natureza qualitativa. Salienta-se a título de exemplo a identificação realizada através da orelha, que é materializada através de uma técnica biométrica que utiliza as características únicas da orelha (curvatura, a posição do lóbulo, a presença de sulcos e dobras, entre outras), sendo possível porque cada indivíduo possui uma forma e tamanho únicos.”
E2	“Primeiramente, assumindo que se tratam de imagens de videovigilância (amostra problema), dificilmente se poderá atingir uma identificação dada a reduzida qualidade das imagens e os detalhes específicos do rosto humano. Ainda assim, tal "identificação de um suspeito" exigiria a realização de uma comparação facial com uma imagem controlada (amostra referência).”
Ideias - chave	A lofoscopia, genética, através da face, da íris, da voz e da morfologia de algumas partes constituintes do corpo humano (por exemplo, a orelha). Através de imagens de videovigilância, dificilmente se poderá atingir uma identificação dada a reduzida qualidade das imagens e os detalhes específicos do rosto humano.

Tabela 2: Apresentação e análise à questão 1

Fonte: Elaboração Própria

5.1.2. Apresentação, análise e discussão da questão nº2

A questão nº 2 “**Até que ponto os olhos poderão ser motivo identificativo?**” tem como objetivo perceber se é possível identificar um ser humano através dos seus olhos.

Em resposta a esta questão o E1 referiu que os olhos podem ser utilizados como característica biométrica para reconhecer/identificar pessoas, no entanto o mesmo não é possível de ser realizado em foro criminal.

O E2 afirmou que os olhos podem contribuir para a criação de uma convicção de identificação, como qualquer outro elemento do rosto, não servindo por isso, para uma identificação precisa e passível de ser usada como prova.

Questão nº2 Até que ponto os olhos poderão ser motivo identificativo?	
Nº	Resposta
E1	“... os olhos podem ser utilizados como característica biométrica para reconhecer/identificar pessoas.” “Contudo, esta utilização ocorre em ambientes controlados e fora do foro criminal. ”
E2	“ Como qualquer outro elemento do rosto podem contribuir para a criação de uma convicção de identificação.”
Ideias - chave	Os olhos podem ser utilizados para identificação de pessoas, contudo atualmente não são utilizados em matéria de foro criminal. Os olhos podem contribuir para a criação de uma convicção de identificação.

Tabela 3: Apresentação e análise à questão 2

Fonte: Elaboração Própria

5.1.3. Apresentação, análise e discussão da questão nº3

A questão nº 3 “**Fazem identificação de suspeitos por imagem CCTV e/ou móvel?**” tem como objetivo perceber se é possível realizar uma identificação de um suspeito através de uma imagem CCTV e/ou móvel.

Tendo em conta o ordenamento jurídico atualmente vigente em Portugal e as capacidades da DIC relativas a esta matéria o E1 responde a esta questão referindo que no âmbito das Ciências Forenses, o reconhecimento e a identificação, embora estejam relacionados, são dois processos distintos. Atualmente, o reconhecimento facial não possui valor probatório absoluto. Pese embora o referido, é possível associar e demonstrar semelhanças em cada estudo, sendo que a convicção do Tribunal para a matéria de facto dada como provada, terá de ter sempre em atenção o disposto no artigo 127.º do CPP, isto é, considerando o princípio de que a prova é apreciada segundo as regras da experiência e a livre convicção, resulta do confronto da prova testemunhal produzida em sede de audiência de discussão e julgamento, prova documental e pericial junta aos autos. Para uma cabal identificação, este procedimento deverá de ser confirmado através de uma perícia (com vista à identificação), realizada por um perito na matéria. Para isso, é feita uma avaliação das imagens para determinar a sua adequação a serem comparadas (determinar semelhanças e diferenças), baseada em critérios assentes em requisitos de qualidade, na sua definição, iluminação, posição do objeto a comparar e a sua visibilidade, entre outros. O estudo (perícia) é expresso sob a forma de correspondências identitária ou graus de uma escala de conclusões que permitem estabelecer resultados, de maior ou menor concordância, na identificação do suspeito. Atualmente, a DIC só possuiu a capacidade de realizar o

reconhecimento, visto ainda não ter peritos para fazer a identificação biométrica, assente neste tipo de características. O reconhecimento/identificação facial utiliza técnicas que permitem comparar as características faciais da pessoa capturada pelas câmaras com as características faciais obtidas através da fotografia técnico-policial de identificação 1 , vulgo cliché. Assim, como referido, caso haja uma correspondência significativa entre as características, é possível realizar a identificação da pessoa em questão, através de uma perícia. No entanto, é importante salientar que o uso destas técnicas depende da qualidade das amostras e da proximidade temporal das mesmas, e deve ser feito com cuidado e em conformidade com as leis e regulamentações aplicáveis à privacidade e à proteção de dados pessoais.

O E2 afirma que não é possível a identificação de suspeitos por imagens não controladas (CCTVs / telemóveis/ redes sociais, etc.)

Questão nº3 Fazem identificação de suspeitos por imagem CCTV e\ou móvel?	
Nº	Resposta
E1	“Atualmente, o reconhecimento facial não possui valor probatório absoluto.” “...terá de ter sempre em atenção o disposto no artigo 127.º do CPP, isto é, considerando o princípio de que a prova é apreciada segundo as regras da experiência e a livre convicção, resulta do confronto da prova testemunhal produzida em sede de audiência de discussão e julgamento, prova documental e pericial junta aos autos.” “... este procedimento deverá de ser confirmado através de uma perícia (com vista à identificação), realizada por um perito na matéria.” “O estudo (perícia) é expresso sob a forma de correspondências identitária ou graus de uma escala de conclusões que permitem estabelecer resultados, de maior ou menor concordância, na identificação do suspeito.” “a DIC só possuiu a capacidade de realizar o reconhecimento, visto ainda não ter peritos para fazer a identificação biométrica, assente neste tipo de características.” “Assim, como referido, caso haja uma correspondência significativa entre as características, é possível realizar a identificação da pessoa em questão, através de uma perícia.” “...deve ser feito com cuidado e em conformidade com as leis e regulamentações aplicáveis à privacidade e à proteção de dados pessoais.”
E2	“Não é possível a identificação de suspeitos por imagens não controladas (CCTVs / telemóveis/ redes sociais, etc.).”
Ideias - chave	O reconhecimento facial resulta no confronto da prova testemunhal produzida em sede de audiência de discussão e julgamento, prova documental e pericial junta aos autos, este é confirmado através de uma perícia. No entanto a DIC não tem capacidade de realizar a identificação de pessoas uma vez que ainda não possui peritos, por isso apenas tem a capacidade de realizar o reconhecimento de pessoas.

Tabela 4: Apresentação e análise à questão 3

Fonte: Elaboração Própria

5.1.4. Apresentação, análise e discussão da questão nº4

A questão nº 4 “**Um reconhecimento positivo neste caso serve como prova ou perícia?**” tem como objetivo perceber se a peritagem feita pelos militares da DIC ou pelos especialistas do LPC em caso de um reconhecimento positivo de um suspeito da prática de um crime serviria em tribunal como prova ou perícia.

Dadas as respostas de ambos os entrevistados, conclui-se que comparando as características biométricas com as características armazenadas numa base de dados de referência é possível associar e demonstrar semelhanças em cada estudo, sendo que a convicção do Tribunal para a matéria de facto essencial.

Questão nº4 Um reconhecimento positivo neste caso serve como prova ou perícia?	
Nº	Resposta
E1	“A identificação é o processo utilizado para estabelecer/determinar a identidade de uma pessoa desconhecida , podendo ser comparadas as suas características biométricas com as características armazenadas numa base de dados de referência . Por outro lado, através do reconhecimento, e pese embora o anteriormente referido, é possível associar e demonstrar semelhanças em cada estudo, sendo que a convicção do Tribunal para a matéria de facto dada como provada, terá de ter sempre em atenção o disposto no artigo 127.º do CPP, isto é, considerando o princípio de que a prova é apreciada segundo as regras da experiência e a livre convicção, resulta do confronto da prova testemunhal produzida em sede de audiência de discussão e julgamento, prova documental e pericial. ”
E2	“ O "reconhecimento positivo, [negativo ou inviável]" servirá como prova ou perícia no que for o entendimento das Autoridades Judiciais (MP e Juiz) e/ou da Defesa, não dos Peritos. ”
Ideias - chave	Comparadas as características biométricas com as características armazenadas numa base de dados de referência, cabe às Autoridades Judiciais dar o seu entendimento relativo às mesmas.

Tabela 5: Apresentação e análise à questão 4

Fonte: Elaboração Própria

5.1.5. Apresentação, análise e discussão da questão nº5

A questão nº 5 “**Qual o procedimento adotado aquando recolhida uma gravação da prática de um crime?**” tem como objetivo perceber qual é o procedimento atualmente utilizado em Portugal aquando recolhida uma gravação da prática de um crime.

Referente a esta questão o E1 afirma que regra geral, a gravação é considerada uma prova do crime e deve ser tratada com cuidado para garantir a sua autenticidade e integridade. Em muitos casos, a gravação é entregue às autoridades policiais, que podem utilizá-la para investigar o crime e com o intuito de identificar os suspeitos. O primeiro elemento policial interveniente no processo (first responder) deverá dar primazia à observação direta das imagens e providenciar uma resposta adequada ao incidente operacional (a observação poderá constituir um precioso auxílio na preservação de zonas potencialmente importantes de conter vestígios, resultante da ação dos suspeitos). Deverá acautelar, previamente, a preservação de todas as imagens necessárias para o processo criminal, para obter informação policial (com vista à descrição da ação e da identificação do(s) autor(es) do ilícito criminal). Usualmente, depois do Órgão de Polícia Criminal (OPC) exercer a proteção cautelar essencial, em resposta ao justo receio (virtual) de dissipação da prova, através de uma

notificação para preservação e entrega de imagens de videovigilância, e de ter em sua posse as imagens, irá realizar a visualização e extração de fotogramas, tentando responder às questões fundamentais da IC. Quando é necessário recorrer às exigências técnico-científicas e métodos específicos na extração (i.e. ampliações e melhoramentos, estudo e/ou comparações de características físicas de indivíduos, de veículos, roupas e objetos, entre outros), considerando a maximização dos recursos da IC-Criminalística, os pedidos de exames/perícias são remetidos, através do fluxo de criminalística, à DIC, do Comando Operacional (CO).

Por outro lado, o E2 refere que quando chega qualquer imagem ao LPC (entenda-se, vestígio) segue-se o procedimento em uso no serviço para recolha de vestígios, através de um fluxograma de friagem, não sendo o mesmo muito preciso na sua resposta.

Questão nº5 Qual o procedimento adotado aquando recolhida uma gravação da prática de um crime?	
Nº	Resposta
E1	“O primeiro elemento policial interveniente no processo deverá dar primazia à observação direta das imagens e providenciar uma resposta adequada ao incidente operacional. Deverá acautelar, previamente, a preservação de todas as imagens necessárias para o processo criminal, para obter informação policial.” “Usualmente, depois do OPC exercer a proteção cautelar essencial, em resposta ao justo receio (virtual) de dissipação da prova, através de uma notificação para preservação e entrega de imagens de videovigilância, e de ter em sua posse as imagens, irá realizar a visualização e extração de fotogramas, tentando responder às questões fundamentais da investigação criminal (IC). Quando é necessário recorrer às exigências técnico-científicas e métodos específicos na extração (i.e. ampliações e melhoramentos, estudo e/ou comparações de características físicas de indivíduos, de veículos, roupas e objetos, entre outros), considerando a maximização dos recursos da IC-Criminalística, os pedidos de exames/perícias são remetidos, através do fluxo de criminalística, à Direção de Investigação Criminal (DIC), do Comando Operacional (CO).”
E2	“...quando nos chega qualquer imagem (entendamos, vestígio) seguimos o Procedimento em uso neste Serviço para recolha de vestígios, através de um fluxograma de friagem.”
Ideias - chave	O primeiro elemento policial interveniente no processo, preserva todas as imagens do processo criminal, visualiza e extrai fotogramas. Pedidos de exames/perícias são remetidos, através do fluxo de criminalística, à DIC.

Tabela 6: Apresentação e análise à questão 5

Fonte: Elaboração Própria

5.1.6. Apresentação, análise e discussão da questão nº6

A questão nº 6 **“O que poderá contribuir para aumentar a eficácia e credibilidade nas identificações positivas de suspeitos quer seja por imagem e\ou som recolhidos no local?”** tem como objetivo perceber que melhorias poderiam ser implementadas para uma melhoria da eficácia e credibilidade nas identificações positivas de suspeitos quer seja por imagem e\ou som recolhidos no local.

Em resposta a esta questão ambos os entrevistados referem que existiria uma melhoria significativa com a utilização de equipamentos de qualidade superior, aumentando a qualidade dos sensores e a capacidade de armazenamento, possuírem melhores enquadramentos e serem alvo de manutenção adequada e frequente.

Contudo, em complemento ao acima exposto, o E1 refere também a importância dos OPC realizarem estudos que permitam identificar os procedimentos competentes e as características mínimas necessárias para os dispositivos de video surveillance system (VSS), que possibilitem legislar sobre os fundamentais atributos técnicos dos equipamentos e a sua correta colocação nos diversos espaços. Complementando ainda, com a sensibilização e a formação adequada dos profissionais envolvidos na recolha (first responders) e análise primária das imagens, e a análise secundária passar a ser realizada por peritos especializados em reconhecimento/identificação facial forense, uma vez que utilizam capacidades técnicas avançadas para identificar e comparar este tipo de características.

Questão nº6 O que poderá contribuir para aumentar a eficácia e credibilidade nas identificações positivas de suspeitos quer seja por imagem e\ou som recolhidos no local?	
Nº	Resposta
E1	“... a utilização de equipamentos de alta qualidade para capturar e gravar imagens mais nítidas e detalhadas, e desta forma convergirem para facilitar a identificação.” “... OPC realizarem estudos que permitam identificar os procedimentos competentes e as características mínimas necessárias para os dispositivos de video surveillance system – VSS, que possibilitem legislar sobre os fundamentais atributos técnicos dos equipamentos, a sua correta colocação nos diversos espaços (através do posicionamento ideal), com vista a aumentar a eficácia e uma captação otimizada das imagens, concorrendo desta forma para que a instalação de videovigilância siga os seus objetivos primordiais, nomeadamente a proteção de pessoas e bens, o seu potencial efeito dissuasor (prevenção) e de controlo de infrações, recolha de provas e por último a identificação biométrica de suspeitos, identificação do perpetrador em processo criminal.” “No que concerne aos OPC, a melhoria poderá passar pela sensibilização e pela formação adequada dos profissionais envolvidos na recolha (first responders) e análise primária das imagens...” “Outra ação, deverá passar pela análise secundária ser realizada por peritos especializados em reconhecimento/identificação facial forense, uma vez que utilizam capacidades técnicas avançadas para identificar e comparar este tipo de características.”
E2	“ De uma forma generalizada — com o alerta que a recolha de áudio não está autorizada em sistemas de videovigilância — as "identificações positivas" teriam ganhos significativos se os sistemas CCTV aumentassem de qualidade dos sensores e da capacidade de armazenamento, que tivessem melhores enquadramentos e que fossem alvo de manutenção adequada e frequente.”
Ideias - chave	Utilização de equipamentos de qualidade superior. Realização de estudos que permitam identificar os procedimentos competentes e as características mínimas necessárias para os dispositivos de video surveillance system – VSS. Sensibilizar e formar adequadamente os “first responders”. A análise secundária ser realizada por peritos especializados em reconhecimento/identificação facial forense.

Tabela 7: Apresentação e análise à questão 6

Fonte: Elaboração Própria

5.2. Análise comparativa a forças congéneres

Este capítulo tem como objetivo realizar uma análise comparativa dos procedimentos adotados por algumas congéneres em matéria de identificação de suspeitos através de sistemas de videovigilância dentro do contexto da presente investigação. A análise comparativa é uma abordagem fundamental para examinar e contrastar diferentes aspetos, características e abordagens relacionadas ao tema em questão. Ao realizar essa análise,

pretendo fornecer uma visão abrangente e aprofundada das várias perspectivas e contribuições existentes nas práticas relacionadas ao tema.

A análise comparativa é uma ferramenta valiosa para identificar semelhanças, diferenças, pontos fortes e limitações nas diferentes abordagens, permitindo uma compreensão mais abrangente do tema estudado. Por meio dessa análise, será possível explorar as nuances, os pontos de convergência e divergência, as lacunas e as oportunidades de avanço na área de pesquisa.

Ao abordar a Royal Netherlands Marechaussee relativamente o tema acima exposto a mesma referiu que utiliza vídeos e imagens de câmeras de vídeo como prova em investigações criminais. Os procedimentos legais diferem dependendo da situação, local e propósito da investigação. Em algumas áreas, os mesmos possuem cobertura permanente de CCTV a partir de sistemas de propriedade das forças policiais. Nesse caso, o uso das imagens e os procedimentos legais necessários são muito mais simples do que, por exemplo, se os vídeos/imagens estiverem armazenados em um servidor privado ou se a câmera/imagens não forem propriedade dos mesmos, como é o caso de shoppings, CCTV municipal local e Campanha de Vídeo RING. Os procedimentos legais são descritos na "Lei de Autorização de Investigação Especial". Essa lei descreve todos os métodos especiais de investigação e o que é necessário para poder usá-los. Geralmente, a autorização deve vir do promotor público ou de um juiz. Tudo depende do grau de invasão da privacidade de alguém. Por exemplo, obter imagens de uma câmera de uma caixa multibanco para a identificação de um suspeito é mais fácil do que obter permissão para instalar uma câmera oculta na casa de alguém por um longo período de tempo para ver se um suspeito visita essa casa. Por fim afirmam, que no caso de uma identificação positiva de um suspeito, isso pode ser adicionado à investigação e se tornar parte dos arquivos disponíveis para o promotor do processo. As imagens recolhidas também podem ser mostradas em tribunal, se necessário.

Da mesma forma, abordando a Arma dei Carabinieri, os mesmos referem que a utilização de dispositivos de videovigilância implica a recolha e armazenamento de informação gráfica ou audiovisual sobre todas as pessoas que entrem no espaço monitorizado, identificáveis pela sua aparência ou outros elementos específicos. A aquisição, gestão e armazenamento das imagens gravadas pelos Carabinieri através da utilização de sistemas de gravação de vídeo digital, para fins de prevenção, investigação, detecção ou repressão de crimes, enquadra-se no disposto na Directiva (UE) 680/2016, transposto pelo ordenamento jurídico italiano com o Decreto Legislativo n.º 51/2018. Os cidadãos, no cumprimento da obrigação de participação, são informados do particular

tratamento de dados pessoais efetuado através de um “aviso de privacidade” especial, em conformidade com o disposto no artigo 42º da Diretiva. Em particular, assegura-se que o tratamento dos dados pessoais seja efetuado com respeito pelos direitos e liberdades fundamentais das pessoas singulares, com especial referência à confidencialidade e ao direito à respetiva proteção. A finalidade do tratamento consiste na recolha e armazenamento de provas áudio-vídeo ou fotográficas relativas a condutas ilícitas, relevantes do ponto de vista criminal ou para aplicação de medidas preventivas, perpetradas em atos ou manifestações públicas. A Garante Privacy deu luz verde ao uso pelos Carabinieri de sistemas de gravação de vídeo digital em serviços de ordem pública e prevenção geral. O esforço organizativo, visando identificar as medidas técnico-organizacionais corretas, permitiu à Autoridade de Supervisão adotar medidas para a aprovação absoluta dos desenhos de processos delineados sobre o tratamento de dados pessoais, os quais foram considerados conformes com os regulamentos da UE.

CONCLUSÕES E RECOMENDAÇÕES

A presente investigação encarou a temática da identificação de suspeitos na Guarda Nacional Republicana com especial foco nos sistemas de videovigilância. No decorrer desta investigação a mesma dividiu-se numa parte teórica onde foi abordado o ordenamento jurídico português relativo ao tema, conceitos inerentes ao mesmo e ainda foi abordado o sistema de reconhecimento facial uma vez que este foi por nós considerado o futuro do reconhecimento de pessoas, e de seguida uma análise prática, onde se procurou perceber procedimentos realizados pela GNR e pelas forças congéneres, nomeadamente Arma dei Carabinieri e a Royal Netherlands Marechaussee, relativo ao tema acima exposto.

Sendo a investigação desenvolvida em torno da QC “Qual a mais-valia para a identificação de suspeitos de crimes para a GNR da utilização imagens e vídeos de sistemas de vídeo vigilância em Portugal?” foi possível retirar elações e adotar posições relativas ao tema da investigação, tendo em conta não só a revisão de literatura efetuada como também através de uma análise de resultados cimentada através de inquéritos por entrevista.

Deste modo, foram levantadas questões no decorrer desta investigação, nomeadamente questões QC e QD’s, as quais são de extrema importância devendo por isso ser respondidas.

Relativamente à QD.1 “Haverá restrições no âmbito legal para a utilização de sistemas de vigilância?” a Lei n.º 95/2021, de 29 de dezembro, que veio regular a utilização pelas forças e serviços de segurança, de sistemas de videovigilância, fazendo relevância no seu artigo 14º para a utilização de sistemas de videovigilância de qualquer entidade pública ou privada, instalados em locais públicos ou privados de acesso ao público nos casos previstos no artigo 3º. Ainda no mesmo artigo é possível verificar que no que toca a matéria de identificação de suspeitos as forças e serviços de segurança podem visualizar as imagens recolhidas pelos sistemas referidos anteriormente, para efeitos de identificação de autor de ilícito criminal, se houver suspeitas que o autor ainda se encontra no local.

No que concerne à QD.2 “Em termos de estudos comparativos o que é que Portugal esta a desenvolver em comparação com os nossos congéneres Europeus?” todos os países europeus são legislados pelo Regulamento (UE) 2016/679 sendo por isso muitos dos procedimentos idênticos em matéria de tratamento de dados pessoais. Contudo, após a

recolha de imagem, a GNR apenas tem a capacidade de efetuar ampliações e melhoramentos, estudo e/ou comparações de características físicas de indivíduos, de veículos, roupas e objetos. Em comparação Instituto Forense da Holanda, atualmente, é prática realizar imagens de reconstrução com suspeitos, sempre que possível, para permitir comparação manual por especialistas. Tendo ainda os mesmos um projeto piloto nos quais modelos 3D são comparados com fotografias 2D, analisando o posicionamento de uma pessoa ou crânio para a comparação de fotos, utilizando análises de três pontos e uma fotografia 3D.

Em resposta à QC “Qual a mais-valia para a identificação de suspeitos de crimes para a GNR da utilização imagens e vídeos de sistemas de vídeo vigilância em Portugal?”, tendo em conta o nosso ordenamento jurídico, é impossível efetuar o reconhecimento de uma pessoa apenas e só através de imagem e/ou vídeo, pois o mesmo tem de ser seguido de uma prova testemunhal presencial. No entanto, não invalida a importância que os sistemas de videovigilância têm em matéria de identificação de suspeitos, uma vez que, mesmo que os mesmos não permitam o reconhecimento da pessoa que praticou o ilícito criminal, revela-se de extrema relevância para a investigação criminal formular uma convicção de investigação.

Pese embora o acima exposto, é de considerar as melhorias que a GNR poderia realizar neste âmbito, começando pela utilização de equipamentos de alta qualidade para capturar e gravar imagens mais nítidas e detalhadas, e desta forma convergirem para facilitar a identificação. Não obstante, a melhoria poderia também passar pela sensibilização e pela formação adequada dos profissionais envolvidos na recolha e análise primária das imagens culminando com uma melhor preservação de prova e continuamente a análise secundária começar a ser realizada por peritos especializados em reconhecimento/identificação facial forense, uma vez que utilizam capacidades técnicas avançadas para identificar e comparar

No que às limitações diz respeito, relevou-se de extrema dificuldade em obter respostas a inquéritos por entrevista às forças congéneres, tendo sido enviados a quatro delas não obtendo nenhuma resposta, conseguindo apenas uma abordagem informal, culminando assim no que considero um aspeto a melhorar no futuro de modo a permitir realizar um estudo comparativo tendo uma maior fundamentação.

Porém, é relevante ressaltar como um aspeto positivo a atualidade do tema, que possibilitou a condução de uma pesquisa enriquecedora, proporcionando um conhecimento aprofundado sobre a legislação atual, os procedimentos adotados pela GNR em relação ao tema e as capacidades que ela possui nessa área.

Para investigações futuras é proposto a realização de um estudo na área do reconhecimento facial e nas potencialidades que tal matéria traria para a GNR.

REFERÊNCIAS BIBLIOGRÁFICAS

- Alves, A. C. (1996). As Forças de Segurança e a Atividade Policial, *Pela Lei Pela Grei*, V, p.5.
- Alves, D. (2017). Métodos, Instrumentos e Técnicas de recolha de dados. Disponível em <https://cienciaeeducacao.com/2017/11/24/metodos-instrumentos-e-tecnicas-de-recolha-de-dado/>.
- Ashby, M. P. (2017). The value of CCTV surveillance cameras as an investigative tool: An empirical analysis. *European Journal on Criminal Policy and Research*, 23, 441- 459.
- Assembleia da República [AR], (1998). Lei no 67/98: Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva no 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados). *Diário da República*.
- Assembleia da República [AR], (2006). Lei n.º 51/2006, de 29 de agosto, *Diário da República*, Série I, n.º 166/2006.
- Assembleia da República [AR], (2007). Lei n.º 33/2007, de 13 de agosto, *Diário da República* Série I, n.º 155/2007.
- Assembleia da República [AR], (2013). Lei n.º 34/2013, de 16 de maio. Estabelece o regime do exercício da atividade de segurança privada e procede à primeira alteração à Lei n.º 49/2008, de 27 de agosto (Lei de Organização da Investigação Criminal). *Diário da República*. n.º 94/2013, I Série. Lisboa, Assembleia da República.
- Assembleia da República [AR], (2021). Lei n.º 95/2021, de 29 de dezembro, *Diário da República*, Série I, n.º 251/2021.
- Assembleia da República [AR]. (2019). Lei n.º 58/2019 de 8 de agosto de 2019. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Diário da República*, 1.ª série, N.º 151.
- Bardin, L. (1977). *Análise de conteúdo*. Lisboa: Edições 70.
- Biblioteca do Instituto Superior Técnico [BIST] (2015). Investigação Científica. Disponível em <https://bist.tecnico.ulisboa.pt/files/sites/37/Investiga%C3%A7%C3%A3oCient%C3%ADfica.pdf>.

- Borg, W. & Gall, M. (2002). *Educational research: An introduction* (7^a ed.) Nova Iorque: Longman.
- Bramble, S., Dr. Compton, D. & KlasÈn, L. (2001). Forensic Image Analysis. In *13th INTERPOL Forensic Science Symposium*, Lyon.
- Brandon, C. W., & Farrington, D. P. (2002). *Crime prevention effects of closed circuit television: a systematic review*, Home Office Research Study 252, Development and Statistics Directorate.
- Bruce, V., Henderson, Z., Greenwood, K., Hancock, P., Burton, M. & Miller, P. (1999) *Verification of Face Identities from Images Captured on Video*, JEP, Applied
- Bryman, A. (2012). *Social Research Methods* (4th Edition). Oxford: Oxford University Press.
- Canotilho, J. J., & Moreira, V. (1993). *Constituição da República Portuguesa Anotada*. Coimbra: Coimbra Editora.
- Carvalho, L. (2015). *Sebenta de Apoio: Metodologias e Técnicas de Investigação*. Universidade Aberta. Lisboa, Portugal.
- Carvalho, M. W. (2013). *Prova por Reconhecimento de Pessoas em Processo Penal*, Dissertação Mestrado em Ciências Jurídico-Forenses, Faculdade de Direito, Universidade de Lisboa, Lisboa.
- Clarke, R. & Weisburd (1994). Diffusion of Crime Control Benefits: Observations on the Reverse of Displacement, em R. V. Clarke (eds.), *Crime Prevention Studies*, NY *Criminal Justice Press*, 2, 165-184.
- Código do Processo Penal. DL n.º 78/87, de 17 de fevereiro. Diário da República, série I, n.º 40.
- Comité dos Direitos Humanos, (2020). Pacto Internacional de Direitos Civis e Políticos. Convenção dos Direitos da Criança, Convenção sobre Eliminação de Todas as Formas de Discriminação contra as Mulheres e a Convenção Internacional sobre os Direitos das Pessoas com Deficiência.
- Constituição da República Portuguesa. *Diário da República*. n.º 86/1976, I série. Lisboa, Assembleia da República.
- Convenção Europeia dos Direitos do Homem, (2017). Lei n.º 65/78 de 13 de outubro. *Concelho da Europa*. Roma, 4.

- Declaração Universal dos Direitos do Homem (DUDH), aprovada pela Assembleia Geral da ONU em 10 de Dezembro de 1948. *Diário da República*, Série I-A, n.º 229/2005.
- Dias, M. G. (1998). *Limites à atuação das forças e serviços de segurança. In Intervenções do seminário internacional Direitos Humanos e eficácia policial: Sistemas de controlo da atividade policial*. Lisboa: IGAI.
- European Forum for Urban Security (2010). *Citizens, Cities and Video Surveillance: Towards a democratic and responsible use of CCTV*. Montreuil.
- Fernandes, L. F. (2006). A prevenção da criminalidade. In M. M. Valente (Coord.), II *Colóquio de Segurança Interna* (pp. 69-115). Coimbra: Edições Almedina.
- Frois, C. (2011), *Vigilância e Poder*, Editora Mundos Sociais, Lisboa.
- Frois, C. (2013). *Peripheral vision: Politics, technology and surveillance*. La Vergne: Berghahn Books.
- Frois, C. (2016, 24 fevereiro). *Interview with C.Frois/ Interviewer: F. Pires. Dos efeitos dos sistemas de videovigilância (CCTV) na criminalidade e sentimento de insegurança da população: Estudo de caso do Bairro Alto*, (Dissertação de Mestrado não publicada). Instituto Superior de Ciências Policiais de Segurança Interna, Lisboa.
- Gabinete do Secretário de Estado da Cultura [GSEC], (2013). Portaria n.º 273/2013, de 13 de maio, *Diário da República*, Série II, n.º 91/2013.
- Gama A., Latas A., Correia J., Lopes J., Triunfante L., Dias M., Mesquita P., Albergaria P., & Milheiro T. (2021). *Comentário Judiciário do Código Processo Penal, Tomo II – art.º 124º a 190º*, 3ª Edição, (pp.331-336), Almedina.
- Gil, A. (2008). *Métodos e técnicas de pesquisa social*. 7ª Edição. São Paulo, Brasil: Atlas.
- Gill, M., Spriggs, A., Argomaniz, J., Bryan, J., Waples, S., Allen, J., Kara, D., Kilworth, J., Little, R., Smith, P., Swain, D. and Jessiman, P. (2005) *Technical: Methods Used in Assessing the Impact of CCTV*, Home Office Online Report, London: Home Office.
- Goold, B. J. (2004). *CCTV and policing: Public area surveillance and police practices in Britain*. Oxford: Oxford University Press.
- Grudin, M. A. (2000). *On Internal Representations in Face Recognition Systems*, *Pattern Recognition* 33, 1161-1177.

- Guerra, A., Pinheiro, A., Barroso, L. D., Campos, E., Geraldês, A. L., & Silveira, L. L. (2004). *Deliberação nº 61/2004 - Princípios sobre o tratamento de dados por videovigilância*. Lisboa: Comissão Nacional de Proteção de Dados.
- Hempel, L., & Töpfer, E. (2002). *Inception report*, Centre for Technology and Society - Technical University Berlin, Berlin.
- Hesseling, René (1994), Displacement: a review of the empirical literature, *Crime Prevention Studies*, 3, 197-230.
- Heuvel, V. D. H., (1998). *Positioning of Persons or Skulls for Photo Comparisons Using Three-Point Analyses and One-Shot 3D Photographs*, Proceedings of SPIE, vol. 3576, pp. 203-215.
- Jeová, M. (2016). Conceitos Básicos de Amostragem. Disponível em <https://petestatistica.github.io/site/download/posts/postJEOVA.html>.
- Johnson, B.R., De Li, S., Larson, D.B., and McCullough, M. (2000). A systematic review of the religiosity and delinquency literature: A research note. *Journal of Contemporary Criminal Justice*, 16, 32-52.
- Jung, C. (2009). Metodologia Científica e tecnológica. Disponível em https://scholar.google.com/citations?view_op=view_citation&hl=th&user=rRgZqU4AAAAJ&citation_for_view=rRgZqU4AAAAJ:OU6Ihb5iCvQC.
- Klare, B., Burge, M., Klontz, J., Bruegge, V. R. & Jain, A., (2012) *Face recognition performance: Role of demographic information*, IEEE Trans. on Information Forensics and Security, 7(6), 1789–1801.
- Klontz, J. C. & Jain, A. K., (2013). *A Case Study on Unconstrained Facial Recognition Using the Boston Marathon Bombings Suspects*, Technical Report MSU-CSE-13-4.
- Ladeira, C. (2006). Iluminação de rua e CCTV: Estudo comparativo. *Revista Polícia e Justiça*, 7, 357-368.
- Madaleno, P. S. J. (2007). *Videovigilância em Locais Públicos – Um novo paradigma da prevenção criminal*. Dissertação (Licenciatura), ISCPSI, Lisboa.
- Matos, J. (2015). Análise documental. Disponível em <http://www.sabercom.furg.br/bitst>
- McLean, S. J., Worden, R. E., & Kim, M. (2013). *Here's looking at you: An evaluation of public CCTV cameras and their effects on crime and disorder*, Criminal Justice Review.
- Mello, R. (2018). Noção de Amostragem. Disponível em https://www.academia.edu/40070657/UNIVERSIDADE_FEDERAL_DO_ESP%C3%8DRITO_S

NATO

_CENTRO_DE_CIENCIAS_AGR%3%81RIAS_E_ENGENHARIAS_DEPART

AME

NTO_DE_ENGENHARIA_RURAL_-

CCAE_RAYANE_LUIZA_DA_SILVA_DE_MEL LO.

Merca, J. A. A. (2021). *Da prova de Reconhecimento, Reconhecimento de Pessoas, Novas Abordagens à Luz da Evolução Científica*, Trabalho Individual Final, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.

Michael, S. (1999). *Volumetric Facial Reconstruction*, PhD Thesis, University of Wales, Swansea.

Ministério da Administração Interna [MAI], (2005). Decreto-Lei n.º 207/2005, de 29 de novembro,

Montgomery, D., Horwitz, S. & Fisher, M., (2013) Police, citizens and technology factor into Boston bombing probe. *The Washington Post*. Acedido a 4 de maio de 2023 em http://articles.washingtonpost.com/2013-04-20/world/386936911_boston-marathon-finish-line-images.

Moreira, L. (2013). *Espaço público, videovigilância e privacidade*. (Dissertação de Mestrado não publicada). ISCTE, Lisboa.

Okabe, R. K. & Carro, S. A. (2014). *Reconhecimento facial em imagens capturadas por câmeras digitais de rede*, Universidade do Oeste Paulista, São Paulo.

Oliveira, J. F. (2006). *As políticas de segurança e os modelos de policiamento: A emergência do policiamento de proximidade*. Coimbra: Almedina.

Pardal, L. & Lopes, S. (2011). *Métodos e técnicas de investigação social*. Porto: Areal Editores.

Phillips, J.P., Grother, P., Michaels, R.J., Blackburn, D.M., Tabassi, E. & Bone, M. (2003). Face recognition vendor test 2002. Acedido a 1 de maio de 2023 em http://www.frvt.org/DLs/FRVT_2002_Evaluation_Report.pdf.

Piza, E. L., Caplan, J. M., & Kennedy, L. W. (2014). CCTV as a tool for early police intervention: Preliminary lessons from nine case studies. *Security Journal*, 30(1), 247-265.

Presidência do Conselho de Ministros [PCM], (2021). Decreto-Lei n.º 87/2021, de 20 de outubro, *Diário da República*, Série I, n.º 204/2021.

- Presidência do Conselho de Ministros [PCM], (2023). Decreto-Lei n.º 2/2023, de 2 de janeiro, *Diário da República*, Série I, n.º 1/2023.
- Prodanov, C. & Freitas, E. (2013). Metodologia do trabalho científico: Métodos e técnicas da pesquisa e do trabalho académico. Disponível em https://books.google.pt/books?hl=ptPT&lr=&id=zUDsAQAAQBAJ&oi=fnd&pg=PA13&dq=m%C3%A9todo+dedutivo+&ots=dc5adwcDO&sig=gtOYFCDJAgMqzSoh6BBaL4_53FM&redir_esc=y#v=onepage&q=m%C3%A9todo%20dedutivo&f=false.
- Quivy, R. & Campenhoudt, L. (1992). *Manual de Investigação em Ciências Sociais*. Lisboa: Gradiva.
- Ratcliffe, J. (2006). *Video surveillance of public spaces. Problem-oriented guides for police: response guides series, 4*, US Department of Justice - Office of Community Oriented Policing Services.
- Ratcliffe, J. (2009). *Problem-oriented guides for police: Guide No. 4 - Video surveillance of public places*. U.S. Department of Justice.
- Reppetto, T. A. (1976). Crime prevention and the displacement phenomenon. *Crime & Delinquency*, 22(2), 166–177.
- Romão, A. (2021). *Definição, Delimitação e Problema*. Academia Militar, Lisboa, Portugal.
- Severino, A. (2013). *Metodologia do Trabalho Científico* (21ª edição). São Paulo, Brasil: Cortez Editora.
- Short, E., & Ditton, J. (1998). Seen and now heard: Talking to the targets of open street CCTV, *The British Journal of Criminology*, 38(3), 404-428.
- Silva, M., Costa, E., Costa, A. (2013). Conhecimento Científico e Sensus Communis: Uma Abordagem Teórica. VII Colóquio Internacional São Cristóvão. Disponível em <https://ri.ufs.br/bitstream/riufs/9718/96/95.pdf>.
- Smith, M., Clarke, R., & Pease, K. (2002). Anticipatory benefits in crime prevention. In N. Tilley (Ed.), *Analysis for crime prevention - Crime Prevention Studies*, 13, 71-88.
- Sousa, J. M. (2009). *Videovigilância e prevenção da criminalidade*, (Dissertação de Mestrado não publicada), Academia Militar, Lisboa.
- Sousa, J., & Baptista, C. (2011). *Como fazer investigação, dissertações, teses e relatórios*. Lisboa: Pactor.

- União Europeia [EU], (2016). Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho de 27 de abril de 2016 relativa à proteção das pessoas singulares, não respeitando o tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de penas, e livre circulação dos dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho. *Jornal Oficial da União Europeia*.
- União Europeia [EU], (2007). Carta dos direitos fundamentais da União Europeia. *Direito e Democracia*, 457.
- União Europeia [EU], (2016). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, 4.
- Uribe, Carlos. (2006). *Derecho a la Intimidad y Videovigilancia Policial*, Laberinto, Madrid.
- Valente, M.M.G. (2012). Capítulo III – Da segurança como tarefa fundamental do Estado de direito democrático. In *Teoria Geral do Direito Policial* (3ª ed.). Coimbra: Almedina.
- Vieira, A. V. M. (2011). *Sistema de Videovigilância – CCTV*. Trabalho de Projeto, Mestrado Integrado em Ciências Policiais, Instituto Superior de Ciências Policiais e Segurança Interna, Lisboa.
- Vilelas, J. (2020). *Investigação. O Processo de Construção do Conhecimento*. Edições Sílabo.
- Welsh, B., & Farrington, D. (2009). Public area CCTV and crime prevention: An updated systematic review and meta-analysis. *Justice Quarterly*, 26(4), 716-745.
- Yoshino, M., Matsuda, H., Kubota, S., Imaizumi, K., & Miyasaka, S. (2000). Computer Assisted Facial Image Identification System using a 3D Physiognomic Range Finder, *Forensic Science International*, vol. 109, nº 3, pp. 225-237.

APÊNDICES

APÊNDICE A – INQUÉRITO POR ENTREVISTA 1



ACADEMIA MILITAR

IDENTIFICAÇÃO DE SUSPEITOS: SISTEMAS DE VIDEOVIGILÂNCIA NA GUARDA NACIONAL REPUBLICANA

Autor: Aspirante de Infantaria da GNR Ricardo Araújo de Almeida Mateus

Orientador: Major de Infantaria da GNR Tiago Silva

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, abril de 2023

CARTA DE APRESENTAÇÃO

O presente estudo, com vista à elaboração do Relatório Científico Final do Trabalho de Investigação Aplicada, na Especialidade de Infantaria da Guarda Nacional Republicana, ministrado na Academia Militar, encontra-se subordinado ao tema “Identificação de suspeitos: Sistemas de videovigilância na guarda nacional republicana”.

Trata-se de uma temática relacionada com a era digital. Neste sentido, pretende-se não só compreender de que maneira é que os sistemas de videovigilância atualmente em uso em Portugal são relevantes para a identificação de suspeitos de crimes como também os procedimentos que são adotados.

Torna-se pertinente, para assegurar a qualidade da investigação, realizar um trabalho de campo baseado em entrevistas. De forma a reunir informações pertinentes relativas à temática abordada, é relevante recolher o depoimento de pessoas ligadas à área, tanto a nível operacional como a nível técnico. A entrevista poderá ser respondida de forma escrita, por via telemática ou de forma presencial.

Face ao exposto, venho por este meio solicitar a Vossa Excelência que me conceda uma entrevista sobre a temática apresentada, pelo que o seu contributo irá acrescentar um elevado valor à investigação.

Grato desde já pela sua disponibilidade e atenção.

Atenciosamente,

Ricardo Araújo de Almeida Mateus
Aspirante de Infantaria da Guarda Nacional Republicana

PROTOCOLO DE CONSENTIMENTO INFORMADO

O presente protocolo é estabelecido entre Ricardo Araújo de Almeida Mateus, aluno da Academia Militar a realizar investigação com o tema “Identificação de Suspeitos: Sistemas de Videovigilância na Guarda Nacional Republicana”, e o participante _____ através do método de entrevista.

O investigador e o orientador científico comprometem-se a:

- a) Conduzir a investigação de acordo com os parâmetros de qualidade preconizados pela comunidade científica da especialidade;
- b) Discutir e negociar outros aspetos específicos de cada caso relativos à confidencialidade da informação, se solicitado pelo participante;
- c) Impedir qualquer divulgação de informação referente aos participantes, exteriormente à equipa de investigação, sem o consentimento prévio de todos os envolvidos;
- d) Entregar uma síntese descritiva dos resultados aos participantes, através de correio eletrónico;
- e) Manter os participantes a par do trabalho que está a ser desenvolvido, nomeadamente no que concerne à análise dos dados, sempre que os mesmos o solicitem;
- f) Prestar aos participantes no processo todos os esclarecimentos solicitados no decorrer da investigação;
- g) Cumprir o Código Deontológico da *American Psychological Association* na realização da investigação;
- h) Eliminar todas as gravações áudio após o decorrer da investigação e a defesa pública da tese.

Os participantes comprometem-se a:

- a) Prestar informações sobre a sua experiência no caso em estudo e sobre a sua experiência profissional;
- b) Ser entrevistado num momento acordado entre o investigador e o participante;
- c) Autorizar a gravação áudio da entrevista, a pedido do investigador;
- d) Decidir mencionar ou omitir a sua participação no projeto nos contextos profissionais em que considere conveniente fazê-lo;
- e) Permitir a publicação do resultado do estudo, com omissão da sua identidade, nomeadamente nas seguintes situações:
 - I. Tese de Mestrado a apresentar à Academia Militar;
 - II. Comunicações em congressos científicos-profissionais;
 - III. Publicações científicas em revistas e/ou em livros da especialidade.

Assinaturas:

(Participante)

(Investigador)

Local e Data:

IDENTIFICAÇÃO DO ENTREVISTADO

Nome:	Hora (Início/Fim):
U/E/O:	Data:
Função/Posto:	Local:

ENTREVISTA

As respostas de Vossa Excelência são fundamentais para atingir os objetivos da investigação, pelo que se solicita que as mesmas sejam o mais completas possível. As suas respostas irão servir única e exclusivamente como objeto de estudo para a investigação, pelo que lhe é solicitada autorização para efetuar gravação e posterior análise e transcrição das respostas (no caso de a entrevista ser presencial). Se for sua intenção, as mesmas ser-lhe-ão facultadas, juntamente com o trabalho final, assim que o mesmo seja aprovado.

Questão 1 – Quais são os sinais característicos que permitem a identificação de um suspeito?

Questão 2 – Até que ponto os olhos poderão ser motivo identificativo?

Questão 3 – Fazem identificação de suspeitos por imagem CCTV e\ou móvel?

Questão 4 – Um reconhecimento positivo neste caso serve como prova ou perícia?

Questão 5 – Qual o procedimento adotado aquando recolhida uma gravação da prática de um crime?

Questão 6 – O que poderá contribuir para aumentar a eficácia e credibilidade nas identificações positivas de suspeitos que seja por imagem e\ou som recolhidos no local?

Muito obrigado pela sua contribuição.

APÊNDICE B – INQUÉRITO POR ENTREVISTA 2



ACADEMIA MILITAR

IDENTIFICAÇÃO DE SUSPEITOS: SISTEMAS DE VIDEOVIGILÂNCIA NA GUARDA NACIONAL REPUBLICANA

IDENTIFICATION OF SUSPECTS: VIDEO SURVEILLANCE SYSTEMS IN THE
REPUBLICAN NATIONAL GUARD

Autor: Aspirante de Infantaria da GNR Ricardo Araújo de Almeida Mateus

Author: Aspirante de Infantaria da GNR Ricardo Araújo de Almeida Mateus

Orientador: Major de Infantaria da GNR (Doutor) Tiago Silva

Advisor: Major de Infantaria da GNR (Doutor) Tiago Silva

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, abril de 2023

COVER LETTER

The present study aims to develop the Final Scientific Report for the Applied Research Work in the Infantry Specialty of the National Republican Guard, taught at the Military Academy, and is focused on the theme "Identification of suspects: Video surveillance systems in the National Republican Guard".

This is a topic related to the digital era. In this sense, the objective is not only to understand how video surveillance systems currently in use in Portugal are relevant for identifying suspects of crimes, but also the procedures that are adopted.

To ensure the quality of the research, it is pertinent to conduct fieldwork based on interviews. In order to gather relevant information related to the topic, it is important to collect the testimony of people connected to the field, both at an operational and technical level. The interview can be answered in writing, via telematics or in-person.

Therefore, I would like to request an interview with Your Excellency on the presented topic, as your contribution will add significant value to the research.

Thank you in advance for your availability and attention.

Sincerely,

Ricardo Araújo de Almeida Mateus
Aspirante de Infantaria da Guarda Nacional Republicana

INFORMED CONSENT PROTOCOL

This protocol is established between Ricardo Araújo de Almeida Mateus, a student at the Military Academy conducting research on the theme "Identification of suspects: Video surveillance systems in the National Republican Guard", and the participant _____ through the method of interview.

The researcher and the scientific advisor commit to:

- i) Conduct the research according to the quality parameters recommended by the scientific community of the specialty;
- j) Discuss and negotiate other specific aspects of each case related to the confidentiality of information, if requested by the participant;
- k) Prevent any disclosure of information concerning the participants outside the research team, without prior consent of all involved;
- l) Deliver a descriptive summary of the results to the participants via email;
- m) Keep the participants informed about the work being developed, especially regarding data analysis, whenever requested;
- n) Provide participants in the process with all the clarifications requested during the research;
- o) Comply with the American Psychological Association's Code of Ethics in conducting the research;
- p) Eliminate all audio recordings after the conclusion of the research and the public defense of the thesis.

The participants commit to:

- f) Provide information about their experience in the case study and their professional experience;
- g) Be interviewed at a time agreed upon between the researcher and the participant;
- h) Authorize the audio recording of the interview, at the request of the researcher;
- i) Decide to mention or omit their participation in the project in professional contexts where they consider it appropriate to do so;
- j) Allow the publication of the study's results, with omission of their identity, particularly in the following situations:
 - I. Master's thesis to be presented at the Military Academy;
 - II. Communications at scientific-professional conferences;
 - III. Scientific publications in specialty journals and/or books

Signatures:

(Participant)

(Investigator)

Location and Date:

INTERVIEWEE IDENTIFICATION

Name:	Hour (Start/End):
Unit:	Date:
Function/Rank:	Location:

INTERVIEW

Your answers are crucial to achieve the objectives of the research, therefore, it is requested that they are as complete as possible. Your answers will be used solely for the purpose of study for the research, and permission is requested to record and later analyze and transcribe the responses (in case of an in-person interview). If you so wish, the same will be provided to you, along with the final work, once it is approved.

1st question – Is it possible to use (as an evidence) images collected by the police of undercover vídeo camaras in criminal investigation? And the images that are collected in CCTV systems?

2nd question– Which are the legal procedures to use the images and recordings of the CCTV systems and other kind of undercover vídeo camaras by the police? Would you tell us if the images of the videocamaras have a good quality to identify a person? Which is the disadvantages of the images colleted through CCTV systems?

3rd question –Is there any *face recognition system* tecnologia on CCTV system?

4th question–In case of a positive identification of a suspect, which is the procedure you follow to be charge in the Court?

5th question– Are there some video surveillance systems controlled and monitored by the police forces? Which are placed it?

6th question – Which kind vídeo camaras are used by the police in the field (Criminal Investigation and other policing areas)?

7th question– Which contributions could be increased to develop the effectiveness and

credibility in terms of identification of the suspects through video surveillance systems?

8th question – Which is the future about identification of suspects through video surveillance systems? Are there some high technologies that the police are testing nowadays that will do a difference in terms of identification of suspects?

Thank you very much for your contribution.

APÊNDICE C – RESPOSTA AO INQUÉRITO POR ENTREVISTA 1 – ENTREVISTADO 1

IDENTIFICAÇÃO DO ENTREVISTADO

Nome: Diogo Almeida e Brito Moreira Dorez

U/E/O: Direção de Investigação Criminal do Comando Operacional

Data: 05/05/2023

Função/Posto: Diretor da DIC / Tenente-Coronel

Local: Alcabideche

Questão 1 – Quais são os sinais característicos que permitem a identificação de um suspeito?

A lofoscopia (impressões datiloscópicas) e a genética (ADN) são duas disciplinas que permitem a identificação de uma pessoa com valor probatório absoluto, uma vez que estas técnicas estudam este tipo de características que são únicas para cada pessoa, logo individualizam o sujeito como uno.

Existem outras características individuais que permitem reconhecer/identificar o ser humano, nomeadamente através da face, da retina, da íris, da voz, da morfologia de algumas partes constituintes do corpo humano, entre outras. Estas características contêm informações únicas de cada indivíduo e podem ser utilizadas para fins de identificação.

O seu estudo tem por base critérios de similitude demonstrativa de natureza qualitativa. Salienta-se a título de exemplo a identificação realizada através da orelha, que é materializada através de uma técnica biométrica que utiliza as características únicas da orelha (curvatura, a posição do lóbulo, a presença de sulcos e dobras, entre outras), sendo possível porque cada indivíduo possui uma forma e tamanho únicos.

Embora a identificação através da orelha seja menos comum do que outras técnicas de biometria, ela pode ser uma opção útil em situações em que as outras características biométricas, como as impressões digitais ou o reconhecimento facial, não são adequadas ou disponíveis. Cada técnica tem as suas próprias vantagens e limitações, e a escolha da técnica adequada dependerá do contexto específico da situação concreta, da qualidade das imagens, das circunstâncias em que se apresentam (características ocultas ou presentes), entre outras.

Questão 2 – Até que ponto os olhos poderão ser motivo identificativo?

Como anteriormente referido, os olhos podem ser utilizados como característica biométrica para reconhecer/identificar pessoas. A título de exemplo, as características únicas da íris e da retina presentes em cada indivíduo já são capturadas e armazenadas em sistemas de reconhecimento ocular, utilizados para autenticação e controlo de acessos em diversas aplicações, edifícios ou infraestruturas, como para a segurança de aeroportos e de sistemas bancários. Contudo, esta utilização ocorre em ambientes controlados e fora do foro criminal.

Questão 3 – Fazem identificação de suspeitos por imagem CCTV e\ou móvel?

No âmbito das Ciências Forenses, o reconhecimento e a identificação, embora estejam relacionados, são dois processos distintos. Atualmente, o reconhecimento facial não possui valor probatório absoluto. Pese embora o referido, é possível associar e demonstrar semelhanças em cada estudo, sendo que a convicção do Tribunal para a matéria de facto dada como provada, terá de ter sempre em atenção o disposto no artigo 127.º do CPP, isto é, considerando o princípio de que a prova é apreciada segundo as regras da experiência e a livre convicção, resulta do confronto da prova testemunhal produzida em sede de audiência de discussão e julgamento, prova documental e pericial junta aos autos.

Para uma cabal identificação, este procedimento deverá de ser confirmado através de uma perícia (com vista à identificação), realizada por um perito na matéria. Para isso, é feita uma avaliação das imagens para determinar a sua adequação a serem comparadas (determinar semelhanças e diferenças), baseada em critérios assentes em requisitos de qualidade, na sua definição, iluminação, posição do objeto a comparar e a sua visibilidade, entre outros. O estudo (perícia) é expresso sob a forma de correspondências identitária ou graus de uma escala de conclusões que permitem estabelecer resultados, de maior ou menor concordância, na identificação do suspeito.

Atualmente, considerando o anteriormente exposto, a DIC só possuiu a capacidade de realizar o reconhecimento, visto ainda não ter peritos para fazer a identificação

biométrica, assente neste tipo de características.

O reconhecimento/identificação facial utiliza técnicas que permitem comparar as características faciais da pessoa capturada pelas câmaras com as características faciais obtidas através da fotografia técnico-policia de identificação, vulgo cliché. Assim, como referido, caso haja uma correspondência significativa entre as características, é possível realizar a identificação da pessoa em questão, através de uma perícia. No entanto, é importante salientar que o uso destas técnicas depende da qualidade das amostras e da proximidade temporal das mesmas, e deve ser feito com cuidado e em conformidade com as leis e regulamentações aplicáveis à privacidade e à proteção de dados pessoais. O reconhecimento de pessoas na União Europeia é regulamentado pelo regulamento geral sobre a proteção de dados (RGPD) e deve ser realizado em conformidade com as regras e regulamentações aplicáveis à proteção de dados pessoais.

Questão 4 – Um reconhecimento positivo neste caso serve como prova ou perícia?

A identificação é o processo utilizado para estabelecer/determinar a identidade de uma pessoa desconhecida, podendo ser comparadas as suas características biométricas com as características armazenadas numa base de dados de referência.

Por outro lado, através do reconhecimento, e pese embora o anteriormente referido, é possível associar e demonstrar semelhanças em cada estudo, sendo que a convicção do Tribunal para a matéria de facto dada como provada, terá de ter sempre em atenção o disposto no artigo 127.º do CPP, isto é, considerando o princípio de que a prova é apreciada segundo as regras da experiência e a livre convicção, resulta do confronto da prova testemunhal produzida em sede de audiência de discussão e julgamento, prova documental e pericial junta aos autos.

Questão 5 – Qual o procedimento adotado aquando recolhida uma gravação da prática de um crime?

Quando uma gravação da prática de um crime é recolhida, o procedimento adotado pode variar de acordo com a situação concreta e a legislação aplicável. No entanto, em geral, a gravação é considerada uma prova do crime e deve ser tratada com cuidado para garantir a sua autenticidade e integridade. Em muitos casos, a gravação é entregue às autoridades policiais, que podem utilizá-la para investigar o crime e com o intuito de

identificar os suspeitos.

O primeiro elemento policial interveniente no processo (first responder) deverá dar primazia à observação direta das imagens e providenciar uma resposta adequada ao incidente operacional (a observação poderá constituir um precioso auxílio na preservação de zonas potencialmente importantes de conter vestígios, resultante da ação dos suspeitos). Deverá acautelar, previamente, a preservação de todas as imagens necessárias para o processo criminal, para obter informação policial (com vista à descrição da ação e da identificação do(s) autor(es) do ilícito criminal).

Usualmente, depois do OPC exercer a proteção cautelar essencial, em resposta ao justo receio (virtual) de dissipação da prova, através de uma notificação para preservação e entrega de imagens de videovigilância, e de ter em sua posse as imagens, irá realizar a visualização e extração de fotogramas, tentando responder às questões fundamentais da investigação criminal (IC).

Quando é necessário recorrer às exigências técnico-científicas e métodos específicos na extração (i.e. ampliações e melhoramentos, estudo e/ou comparações de características físicas de indivíduos, de veículos, roupas e objetos, entre outros), considerando a maximização dos recursos da IC-Criminalística, os pedidos de exames/perícias são remetidos, através do fluxo de criminalística, à Direção de Investigação Criminal (DIC), do Comando Operacional (CO).

É importante ressaltar que a obtenção deste tipo de gravações pode estar sujeita a regulamentações específicas (i.e. Lei n.º 109/2009, de 15 de setembro - Lei do Cibercrime).

Questão 6 – O que poderá contribuir para aumentar a eficácia e credibilidade nas identificações positivas de suspeitos que seja por imagem e/ou som recolhidos no local?

Existem algumas medidas que podem contribuir para aumentar a eficácia e credibilidade dos reconhecimentos/identificações de suspeitos com base em imagens recolhidas nos diversos locais de crime.

Algumas dessas medidas incluem a utilização de equipamentos de alta qualidade para capturar e gravar imagens mais nítidas e detalhadas, e desta forma convergirem para facilitar a identificação.

Outra das medidas poderá consistir em os OPC realizarem estudos que permitam identificar os procedimentos competentes e as características mínimas necessárias para os dispositivos de video surveillance system – VSS, que possibilitem legislar sobre os

fundamentais atributos técnicos dos equipamentos, a sua correta colocação nos diversos espaços (através do posicionamento ideal), com vista a aumentar a eficácia e uma captação otimizada das imagens, concorrendo desta forma para que a instalação de videovigilância siga os seus objetivos primordiais, nomeadamente a proteção de pessoas e bens, o seu potencial efeito dissuasor (prevenção) e de controlo de infrações, recolha de provas e por último a identificação biométrica de suspeitos, identificação do perpetrador em processo criminal.

No que concerne aos OPC, a melhoria poderá passar pela sensibilização e pela formação adequada dos profissionais envolvidos na recolha (first responders) e análise primária das imagens, visto que estas ações podem garantir que os procedimentos sejam realizados com precisão e consistência, aumentando assim a eficácia dos reconhecimentos/identificações positivas.

Outra ação, deverá passar pela análise secundária ser realizada por peritos especializados em reconhecimento/identificação facial forense, uma vez que utilizam capacidades técnicas avançadas para identificar e comparar este tipo de características.

APÊNDICE D – RESPOSTA AO INQUÉRITO POR ENTREVISTA 1 – ENTREVISTADO 2

IDENTIFICAÇÃO DO ENTREVISTADO

Nome: Carlos Gregório

U/E/O: Laboratório de Polícia Científica

Data: 10/05/2023

Função/Posto: Especialista de Polícia Científica

Local: Sede Polícia Judiciária, Lisboa

Questão 1 — Quais são os sinais característicos que permitem a identificação de um suspeito?

Primeiramente, assumindo que se tratam de imagens de videovigilância (amostra problema), dificilmente se poderá atingir uma identificação dada a reduzida qualidade das imagens e os detalhes específicos do rosto humano. Ainda assim, tal "identificação de um suspeito" exigiria a realização de uma comparação facial com uma imagem controlada (amostra referência).

Questão 2 — Até que ponto os olhos poderão ser motivo identificativo?

Como qualquer outro elemento do rosto podem contribuir para a criação de uma convicção de identificação.

Questão 3 — Fazem identificação de suspeitos por imagem CCTV e/ou móvel?

Não é possível a "identificação de suspeitos" por imagens não controladas (CCTVs / telemóveis/ cedes sociais, etc.).

Questão 4 — Um reconhecimento positivo neste caso serve como prova ou perícia?

O "reconhecimento positivo, [negativo ou inviável]" servirá como prova ou perícia no que for o entendimento das Autoridades Judiciais (MP e Juiz) e/ou da Defesa, não dos Peritos.

Questão 5 — Qual o procedimento adotado aquando recolhida uma gravação da prática de um crime?

Questão muito vaga, mas quando nos chega qualquer imagem (entendamos, vestígio) seguimos o Procedimento em uso neste Serviço para recolha de vestígios, através de um fluxograma de friagem.

Questão 6 — O que poderá contribuir para aumentar a eficácia e credibilidade nas identificações positivas de suspeitos que seja por imagem e/ou som recolhidos no local?

De uma forma generalizada — com o alerta que a recolha de áudio não está autorizada em sistemas de videovigilância — as "identificações positivas" teriam ganhos significativos se os sistemas CCTV aumentassem de qualidade dos sensores e da capacidade de armazenamento, que tivessem melhores enquadramentos e que fossem alvo de manutenção adequada e frequente.