ACADEMIA MILITAR

Os desafios da videovigilância policial em espaços públicos

Autor: Aspirante de GNR Infantaria Gonçalo Tibério Faria

Orientador: Tenente-Coronel de Infantaria Renato Pessoa dos Santos

Coorientador: Major de Infantaria da GNR Gonçalo Nuno Correia Zambujo Serrão

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Dissertação de Mestrado

Lisboa, maio de 2023

ACADEMIA MILITAR

Os desafios da videovigilância policial em espaços públicos

Autor: Aspirante de GNR Infantaria Gonçalo Tibério Faria

Orientador: Tenente-Coronel de Infantaria Renato Pessoa dos Santos

Coorientador: Major de Infantaria da GNR Gonçalo Nuno Correia Zambujo Serrão

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Dissertação de Mestrado

Lisboa, maio de 2023

EPÍGRAFE

"Discovery consists of seeing what everybody has seen
and thinking what nobody has thought."
- Albert Szent-Györgyi

DEDICATÓRIA

Ao meu pai (*in memoriam*).

À minha mãe.

Aos meus irmãos.

À minha namorada.

AGRADECIMENTOS

Gostaria de expressar os meus sinceros agradecimentos a todas as pessoas que contribuíram para o sucesso deste trabalho de investigação, tanto academicamente, bem como pelo apoio que me foi prestado ao longo dos anos, não só na realização desta tarefa, mas na minha carreira militar, e especialmente durante o Curso de Formação de Oficiais da GNR.

Ao meu Orientador, Tenente-Coronel Renato Pessoa dos Santos, que prontamente respondeu às minhas solicitações de apoio, pela sua entrega e motivação ao longo desta investigação. Fruto da sua experiência, prestou um apoio significativo na estrutura e metodologia utilizada.

Ao Coorientador, Major Nuno Correia Zambujo Serrão, que acompanhou atentamente o desenvolvimento da investigação, dissipando dúvidas e compartilhando valiosos conhecimentos sobre o assunto, e ainda, pelo apoio prestado com a sua rede de contactos, os quais esta investigação não seria possível.

A todos os entrevistados, pela disponibilidade e também pela partilha de conhecimentos e experiência, contribuindo com dados fundamentais para este RFCTIA.

À minha mãe, ao meu pai (*in memoriam*) e aos meus irmãos, pelo amor incondicional que transmitem todos os dias, tudo o que será alcançado por mim, será sempre uma vitória deles. Ao resto da minha família, que sempre me prestou apoio em qualquer momento. E à minha namorada, pelo amor, pela motivação, e pelo apoio com entusiamo constante, e que me incentiva a lutar por ser alguém melhor todos os dias.

Aos meus camaradas do XXVIII Curso de Formação de Oficiais da GNR, pela camaradagem, união, espírito de sacrifício e espírito de corpo demonstrado ao longo destes cinco anos.

A todos, o meu sincero Obrigado!

RESUMO

Em Portugal é possível verificar-se que a videovigilância policial em espaços públicos apresenta desafios significativos. Este estudo destaca a importância de encontrar um equilíbrio entre a segurança pública e a proteção dos direitos individuais na aplicação dos sistemas de videovigilância policial em espaços públicos. O presente estudo teve como objetivo avaliar os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos.

Identificaram-se desafios, como a necessidade de pareceres da CNPD para fundamentar a utilização dos sistemas, a manutenção e renovação tecnológica, e a busca por soluções adequadas para garantir a segurança da sociedade. A pesquisa contribuiu para um melhor entendimento desses sistemas e para a perceção dos desafios envolvidos, ressalvando a importância da continuidade do debate e da realização de estudos futuros, incluindo a comparação com sistemas de videovigilância de forças de segurança internacionais, para informar o contexto português de acordo com a legislação vigente.

Ao analisar o ordenamento jurídico nacional, constatou-se a existência de regulamentações específicas que estabelecem as condições e limites para a implantação e operação dos sistemas de videovigilância policial. Essas regulamentações desempenham um papel fundamental na proteção dos direitos individuais e na preservação da privacidade dos cidadãos. Através de uma análise detalhada das leis e regulamentos pertinentes, foi possível obter uma compreensão abrangente do quadro jurídico que orienta a videovigilância policial em espaços públicos.

Além disso, a pesquisa explorou o espectro de aplicações tecnológicas disponíveis para esses sistemas. Isso incluiu sistemas de monitorização em tempo real e análise de vídeo, reconhecimento facial e deteção de comportamentos e objetos suspeitos. Essas tecnologias mostraram um potencial significativo para aumentar a eficácia e a eficiência da segurança pública. No entanto, também levantaram questões éticas e preocupações relacionadas com o uso adequado dos dados pessoais e à possibilidade de discriminação algorítmica.

A viabilidade da IA nos sistemas de videovigilância policial em espaços públicos foi investigada, reconhecendo tanto os benefícios quanto os desafios associados. A IA pode aprimorar a deteção de atividades suspeitas e melhorar a capacidade de resposta das forças policiais. No entanto, é essencial abordar questões éticas, garantir a transparência e a prestação de contas, além de evitar a amplificação de vieses e discriminação algorítmica.

Em conclusão, este estudo abordou de forma abrangente os desafios da videovigilância policial em espaços públicos. Ao examinar o ordenamento jurídico nacional, explorar as aplicações tecnológicas e investigar a viabilidade da IA, foi possível compreender as complexidades desse campo e destacar a importância de um equilíbrio entre a segurança pública e a proteção dos direitos individuais. É essencial equilibrar os benefícios da previsão e prevenção de crimes com o respeito dos direitos fundamentais dos cidadãos.

Esta pesquisa contribuiu para um melhor entendimento dos sistemas de videovigilância e como estão a ser aplicados. Além disso, proporcionou uma perceção dos desafios inerentes à aplicação desses sistemas em espaços públicos, procurando um equilíbrio adequado entre a segurança e a proteção dos direitos pessoais.

No entanto, é importante ressaltar algumas limitações encontradas durante o desenvolvimento desta investigação. A escassez de especialistas nesta área foi uma das principais limitações, o que resultou em entrevistas limitadas com indivíduos com conhecimento e experiência. Para pesquisas futuras, sugere-se a realização de estudos comparativos com forças de segurança internacionais congéneres às portuguesas, a fim de conhecer seus sistemas de videovigilância e entender como podem ser aplicados no contexto português, de acordo com a legislação em vigor.

Em suma, o grande desafio enfrentado atualmente é encontrar soluções que permitam o uso eficiente da tecnologia existente, ao mesmo tempo em que se garantem mecanismos adequados de proteção de dados pessoais. Para isso, é necessário investir em políticas e regulamentações que estabeleçam diretrizes claras sobre o uso e o acesso a informações sensíveis, conciliando a eficácia na prevenção e combate ao crime com a preservação dos direitos individuais. Essa busca por soluções equilibradas deve ser realizada por meio de um debate amplo e aberto, envolvendo diversos setores da sociedade e especialistas, a fim de maximizar os benefícios da tecnologia e minimizar as suas potenciais vulnerabilidades.

Palavras-chave: Videovigilância, GNR, Inteligência Artificial, Policiamento

ABSTRACT

In Portugal, it is possible to observe significant challenges in the use of police video surveillance in public spaces. This study emphasizes the importance of finding a balance between public security and the protection of individual rights in the implementation of police video surveillance systems in public areas. The objective of this study was to assess the inherent challenges in the application of police video surveillance systems in public spaces.

Challenges were identified, such as the need for opinions from the National Data Protection Commission (CNPD) to support the use of these systems, technological maintenance and upgrades, and the search for appropriate solutions to ensure societal safety. The research contributed to a better understanding of these systems and the perception of the involved challenges, emphasizing the importance of ongoing debate and future studies, including comparisons with video surveillance systems used by international law enforcement agencies, to inform the Portuguese context in accordance with current legislation.

By analyzing the national legal framework, specific regulations were found that establish the conditions and limits for the deployment and operation of police video surveillance systems. These regulations play a fundamental role in protecting individual rights and preserving citizens' privacy. Through a detailed analysis of relevant laws and regulations, a comprehensive understanding of the legal framework guiding police video surveillance in public spaces was obtained.

Additionally, the research explored the spectrum of technological applications available for these systems. This included real-time monitoring and video analysis, facial recognition, and detection of suspicious behaviors and objects. These technologies showed significant potential to enhance the effectiveness and efficiency of public security. However, they also raised ethical concerns and issues related to the proper use of personal data and the potential for algorithmic discrimination.

The feasibility of AI in police video surveillance systems in public spaces was investigated, acknowledging both the benefits and challenges associated with its use. AI can enhance the detection of suspicious activities and improve the responsiveness of law enforcement agencies. However, it is essential to address ethical issues, ensure transparency and accountability, and avoid the amplification of biases and algorithmic discrimination.

In conclusion, this study comprehensively addressed the challenges of police video surveillance in public spaces. By examining the national legal framework, exploring technological applications, and investigating the feasibility of AI, it was possible to understand the complexities of this field and highlight the importance of balancing public security with the protection of individual rights. It is essential to strike a balance between the benefits of crime prediction and prevention and the respect for citizens' fundamental rights.

This research contributed to a better understanding of video surveillance systems and their implementation. Furthermore, it provided insight into the challenges inherent in the application of these systems in public spaces, seeking an appropriate balance between security and the protection of personal rights.

However, it is important to note some limitations encountered during the development of this research. The scarcity of experts in this field was one of the main limitations, resulting in limited interviews with individuals knowledgeable and experienced in the subject matter. For future research, it is suggested to conduct comparative studies with international law enforcement agencies similar to those in Portugal to learn about their video surveillance systems and understand how they can be applied in the Portuguese context, in accordance with current legislation.

In summary, the current major challenge is to find solutions that enable the efficient use of existing technology while ensuring adequate mechanisms for the protection of personal data. To achieve this, investment in policies and regulations that establish clear guidelines on the use and access to sensitive information is necessary, reconciling effectiveness in crime prevention and combat with the preservation of individual rights. This search for balanced solutions should be carried out through broad and open debate, involving various sectors of society and experts, to maximize the benefits of technology and minimize its potential vulnerabilities.

Keywords: Video surveillance, GNR, Artificial Intelligence, Policing

ÍNDICE GERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

LISTA DE APÊNDICES E ANEXOS

LISTA DE ABREVIATURAS, SIGLAS E ACRÓNIMOS

art.	Artigo
CEDH	Convenção Europeia dos Direitos Humanos
CRP	Constituição da República Portuguesa
DUDH	Declaração Universal dos Direitos Humanos
FFSS	Forças e Serviços de Segurança
n.	Número
RGPD	Regulamento Geral sobre a Proteção de Dados
UE	União Europeia
CE	Comissão Europeia
DLG	Direitos Liberdades e Garantias
PE	Parlamento Europeu

INTRODUÇÃO

A presente Dissertação de Mestrado, que conclui o ciclo de estudos no Mestrado Integrado em Ciências Militares, especialidade Segurança, na Academia Militar, subordina-se ao tema "Os desafios do avanço tecnológico dos sistemas de videovigilância policial em espaços públicos".

Esta investigação tem como objetivo analisar os desafios do avanço tecnológico dos sistemas de videovigilância utilizados pelas forças policiais em espaços públicos, levando em consideração não apenas a evolução tecnológica dos sistemas, mas também o ordenamento jurídico em vigor, tanto internacional como da União Europeia e nacional. Ao abordar essa questão, pretende-se contribuir para o debate sobre como equilibrar a necessidade de proteger a segurança pública com a proteção da vida privada, fornecendo novas perspetivas e *insights* valiosos para a sociedade como um todo. Serão discutidas as aplicações tecnológicas dos sistemas de videovigilância, incluindo a sua evolução, a videovigilância policial, a utilização de Inteligência Artificial (IA) e a aplicabilidade desses sistemas.

Em Portugal, como refere Pereira, (2019), existem casos em que legalmente é estabelecido uma obrigatoriedade na utilização destes sistemas, como por exemplo, nos postos de combustível, bancos, farmácias; entre outros setores. É de especial relevância referir a Lei n.º 95/2021, de 29 de dezembro, que revoga a Lei n.º 1/2005, de 10 de janeiro, que regulava a utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum. Essa lei permitia o uso desses sistemas pela Guarda Nacional Republicana (GNR), Polícia de Segurança Pública e outras entidades responsáveis pela prevenção e investigação criminal.

A utilização de sistemas de videovigilância policial em espaços públicos é um tema de grande importância social, pois afeta diretamente tanto a privacidade como a segurança dos cidadãos. Em muitos países, o uso desses sistemas tem se expandido rapidamente, sendo justificado pelas autoridades como uma medida essencial para a prevenção e combate ao crime, com o avanço da tecnologia, esses sistemas tornaram-se mais sofisticados e capazes de monitorizar maiores quantidades de informações em tempo real. No entanto, apesar dos benefícios que esses sistemas podem trazer para a segurança pública, essa expansão também tem gerado preocupações e críticas por parte de especialistas em direitos humanos, que

argumentam que os sistemas de videovigilância podem invadir a privacidade e representar uma ameaça à liberdade e proteção de dados pessoais.

Na Academia Militar, o ciclo de estudos é concluído por meio da elaboração de uma dissertação de mestrado, que resulta na obtenção do grau de mestre e na especialização académica do aluno, por meio da atividade de pesquisa. Assim escolha do tema de uma dissertação deve atender a uma série de critérios, incluindo a atualidade e a inovação do tema, bem como a sua relevância para as motivações do investigador (Sarmento, 2013). O motivo da escolha deste tema é fundamentado pelo crescente avanço tecnológico em torno da Inteligência Artificial, que, em conjunto com os sistemas de videovigilância tornam esta um excelente instrumento de apoio à prevenção e repressão criminal. E ainda, em Portugal, a videovigilância é um assunto que ainda não é amplamente estudado, por esse motivo existem poucos locais de espaço público em que existem estes sistemas controlados pelas policias, nomeadamente a GNR garante segurança, com o apoio de câmaras de videovigilância, em Fátima, algumas regiões florestais também são controladas com estes meios, e ainda está aprovado para a região de Albufeira a utilização desta ferramenta, e sendo esta uma excelente ferramenta de apoio, deve ser estudada para que o trabalho das forças de segurança seja mais efetivo e consiga dar ao cidadão uma resposta mais célere.

Portanto, a relevância e atualidade deste estudo são evidentes, uma vez que o tema da videovigilância policial em espaços públicos é tanto controverso quanto pertinente, trata-se de um tema que tem gerado discussões e debates em várias partes do mundo, dada a sua complexidade e as implicações para a privacidade, segurança e liberdade individual. O uso dessa tecnologia está em constante evolução e é necessário que sejam realizadas investigações para avaliar tanto a sua eficácia, como para identificar possíveis riscos e desafios. Dessa forma, esta pesquisa tem o objetivo de contribuir para um debate informado e sustentado sobre a videovigilância policial em espaços públicos, oferecendo uma análise crítica e construtiva sobre o tema.

Assim sendo, o objetivo geral deste tipo de investigação deve estar relacionado a uma compreensão ampla e abrangente da temática, englobando o cerne dos fenómenos e ideias estudados (Prodanov & Freitas, 2013). Desse modo, pressupõe-se que qualquer investigação deve ter um objetivo claro, definindo o que se pretende procurar e alcançar (Lakatos & Marconi, 2003). Foi então definido o seguinte objetivo geral (OG) desta investigação:

OG: Avaliar os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos.

Para chegar ao objetivo geral, é necessário determinar objetivos específicos (OE) de carácter mais concreto (Prodanov & Freitas, 2013). Assim o objetivo geral foi repartido em três objetivos específicos, de forma a criar uma linha de pensamento lógica, contruindo um estudo bem estruturado:

OE1: Analisar o ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos.

OE2: Analisar o espectro de aplicações tecnológicas que podem ser utilizadas em sistemas de videovigilância policial em espaços públicos.

OE3: Investigar a aplicabilidade da Inteligência Artificial nos sistemas de videovigilância policial em espaços públicos.

De forma a cumprir os objetivos, deve ser estabelecida uma pergunta de partida. Vem nos dizer Quivy e Campenhout (2005) que, para se transmitir de forma clara, exequível e pertinente o propósito de uma investigação, é imperativo a elaboração de uma pergunta de partida (PP), como tal, o investigador procura expressar com a maior precisão possível o que pretende saber, esclarecer e compreender melhor, essa pergunta servirá como o primeiro fio condutor da investigação. Então, para se procurar aplicações tecnológicas para serem implementadas nos sistemas de videovigilância, formulou-se a seguinte pergunta de partida:

PP. *Quais são os principais desafios enfrentados na aplicação dos sistemas de videovigilância policial em espaços públicos?*

Esta dissertação está articulada em três capítulos. No Capítulo 1 fez-se um levantamento do ordenamento jurídico referente aos sistemas de videovigilância com um enquadramento do direito internacional, a que Portugal está sujeito, onde a própria Constituição da República Portuguesa (CRP) assim o define. Ainda no âmbito internacional, e estando Portugal inserido na União Europeia, o direito aplicável é conceituado à luz das normas e princípios estabelecidos pelo ordenamento jurídico da União Europeia. Por fim, neste capítulo, é referida a legislação nacional que tem forte impacto na utilização dos sistemas de videovigilância, quer pelas possibilidades que as normas apresentam, quer pelas limitações à sua implementação, e ainda a todo o processo que a aplicação destes sistemas está sujeito.

No Capítulo 2 procurou-se entender o estado da arte no que concerne à videovigilância, elucidando as várias fases da sua evolução, e de seguida, para se entender melhor o objeto de estudo, fez-se a conceptualização da videovigilância policial, assim como o da inteligência artificial, onde esta investigação também incidiu. O capítulo termina com as possibilidades e potencialidades que podem ser obtidas, se os sistemas de videovigilância

estiverem em si incorporados elementos de inteligência artificial, onde são abordados a prevenção, a utilização de dados biométricos, ou reconhecimento facial, e a analítica de vídeo.

Encerrando o enquadramento teórico, o Capítulo 3 faz uma abordagem ao conceito de IA, definindo diversos conceitos que devem ser tidos em conta nesta temática. Ainda neste capítulo, foi explorada a interseção entre a IA e dois aspetos cruciais para a temática, primeiramente a videovigilância e, de seguida, a proteção dos dados pessoais.

PARTE I – ENQUADRAMENTO TEÓRICO

CAPÍTULO 1 – ORDENAMENTO JURÍDICO

1.1. Enquadramento

Para se falar de videovigilância, é imperativo abordar os dados pessoais e o seu tratamento, sendo que é disso que te trata quando se captura a imagem ou som das câmaras de videovigilância, conforme define a Lei n.º 59/2019, de 8 de agosto, art.º 3º, al. c), **dados pessoais** entende-se por "informações relativas a uma pessoa singular identificada ou identificável" (AR, 2019b, p. 41), e o seu **tratamento**, al. d) do mesmo artigo, refere-se à atividade ou conjunto de atividades realizadas sobre dados pessoais ou conjuntos de dados pessoais, de forma automatizada ou não automatizada, essas atividades podem incluir "a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, por difusão ou por qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição" (AR, 2019b, p. 41). Assim, revela a importância da presente investigação, abordar os normativos referentes aos Direitos, Liberdades e Garantias (DLG) das pessoas, inclusive do seu direito à privacidade, e proteção de dados pessoais.

Apesar dos documentos internacionais a seguir mencionados não abordarem diretamente o tema da videovigilância, é importante mencioná-los, uma vez que a imagem capturada pela videovigilância pode identificar uma pessoa e, portanto, constitui um dado pessoal. Esses documentos representam importantes diretrizes que têm influenciado a legislação ordinária sobre a videovigilância e sobre a proteção dos dados pessoais, portanto devem ser considerados.

O tema em análise, relacionada à possibilidade de adoção de um sistema de videovigilância em espaço público, envolve uma série de questões importantes relacionadas aos DLG dos cidadãos. É necessário equilibrar a necessidade de proteção da segurança pública e a proteção da privacidade e dos direitos individuais. É responsabilidade do poder político garantir a justiça e a segurança de seus cidadãos, e há uma relação estratégica entre a política e a segurança, que são conceitos independentes na investigação das questões e desafios enfrentados por qualquer Estado moderno (Correia & Duque, 2012).

Devido à importância da questão, a legislação aplicável inclui não apenas as leis internas de cada país, mas também legislação internacional e comunitária que têm tido influência significativa na legislação ordinária nessa área. Por exemplo, a Declaração

Universal dos Direitos Humanos (DUDH) e o Pacto Internacional sobre Direitos Civis e Políticos garantem o direito à privacidade e à proteção contra interferências arbitrárias na vida privada. A Convenção Europeia dos Direitos Humanos também protege o direito à privacidade e estabelece que qualquer interferência deve ser justificada por razões legais e ser necessária em uma sociedade democrática (Rodrigues, 2022).

Além disso, a Diretiva da União Europeia (UE) sobre proteção de dados pessoais, conhecida como Regulamento Geral sobre a Proteção de Dados (RGPD), estabelece uma série de regras para o processamento de dados pessoais, incluindo imagens de vídeo. Essa diretiva é aplicável a todas as entidades que operam dentro da UE, independentemente do local onde os dados são processados (Pereira, 2019).

A legislação interna de cada país é a principal reguladora da videovigilância. Em geral, as leis nacionais estabelecem limites para a videovigilância em espaços públicos, incluindo requisitos para informar as pessoas que estão sendo filmadas, limitações de tempo para a retenção de dados e restrições ao uso de imagens para fins não relacionados à segurança pública (Albuquerque, 2022)

Em suma, a regulamentação da videovigilância é complexa e deve ponderar uma série de aspetos, incluindo a proteção da privacidade e dos dados pessoais. A legislação interna de cada país deve ser complementada por leis internacionais e comunitárias relevantes para garantir que as restrições aos direitos dos cidadãos sejam criteriosamente reguladas pela Lei.

1.2. Direito Internacional

Para se estudar o direito internacional referente aos sistemas de videovigilância é necessário primeiramente trazer à colação a proteção de dados, os DLG dos cidadãos, e consequentemente a videovigilância, a partir da eventual captura de imagem e som. Assim, como referido anteriormente, a problemática em estudo diz respeito à admissibilidade e implementação de sistemas de videovigilância em espaços públicos, que envolvem restrições aos DLG dos cidadãos, conforme estabelecidos na Constituição da República Portuguesa (CRP). Portanto, é crucial que essas restrições sejam regulamentadas cuidadosamente pela Lei, definindo claramente o alcance e os limites dessas medidas de vigilância. Assim, e de acordo com a CRP, no seu art.º 8º, no n.º 1 “as normas e os princípios de direito internacional geral ou comum fazem parte integrante do direito português”, incluindo o que vem explícito no n.º 2 “as normas constantes de convenções internacionais regularmente ratificadas ou aprovadas vigoram na ordem interna após a sua publicação oficial e enquanto vincularem internacionalmente o Estado Português“, e ainda o n.º 3 “as

normas emanadas dos órgãos competentes das organizações internacionais de que Portugal seja parte vigoram directamente na ordem interna, desde que tal se encontre estabelecido nos respectivos tratados constitutivos" (AR, 1976).

Em matéria de proteção, importa referir a Declaração Universal dos Direitos Humanos (DUDH) no seu art.º 12º, que estabelece o seguinte: "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação" (Assembleia Geral da Organização das Nações Unidas, 1948).

Neste âmbito vale ressalvar também o Pacto Internacional sobre Direitos Civis e Políticos, aprovado para ratificação no ordenamento jurídico português através da Lei n.º 29/78, de 12 de junho, é um tratado internacional de direitos humanos que estabelece normas e padrões para a proteção dos direitos civis e políticos de todas as pessoas, em particular, o art.º 17º do pacto estabelece que "Ninguém poderá ser objeto de ingerências arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de ataques à sua honra e reputação" (Assembleia Geral da Organização das Nações Unidas, 1966). Esse artigo reconhece o direito fundamental à privacidade, protegendo os cidadãos contra a invasão indevida da sua vida privada, por parte do Estado ou de terceiros. Estabelece também que, qualquer interferência na vida privada de uma pessoa deve ser legalmente prevista, necessária e proporcional aos objetivos legítimos perseguidos, garantindo assim a proteção da dignidade e dos direitos fundamentais de cada indivíduo (Moleirinho, 2021).

Portanto, o Pacto Internacional sobre Direitos Civis e Políticos desempenha também um papel importante na proteção dos direitos humanos, incluindo o direito à privacidade e à proteção de dados pessoais. Este estabelece padrões mínimos que os Estados devem cumprir para garantir que as medidas de vigilância sejam legais, proporcionais e necessárias para proteger a segurança e os interesses públicos, ao mesmo tempo em que respeitam os direitos fundamentais dos indivíduos (Veiga, 2020).

1.3. Direito Comunitário

Além da DUDH e do Pacto Internacional sobre Direitos Civis e Políticos, existem outros instrumentos internacionais relevantes para a proteção dos direitos humanos no contexto da videovigilância. No âmbito da temática em questão, é importante salientar também os normativos vigente na UE.

Um exemplo é a Convenção Europeia dos Direitos Humanos (CEDH) (Conselho da Europa, 1950), que também reconhece o direito à privacidade e estabelece requisitos para a

legalidade e a proporcionalidade das medidas de vigilância. A Convenção exige que a vigilância seja "necessária em uma sociedade democrática" e que seja acompanhada por salvaguardas adequadas para garantir que os indivíduos afetados possam exercer seus direitos. No art.º 8º, n.º 1 refere a CEDH que "qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência", ainda no seu n. º 2, a autoridade pública não pode interferir no exercício deste direito, a não ser nos casos em que esteja legalmente prevista a interferência, e que seja considerada necessária numa sociedade democrática para garantir a segurança nacional, a segurança pública, o bem-estar económico do país, a manutenção da ordem, a prevenção de infrações penais, a proteção da saúde ou da moral, bem como a proteção dos DLG(Conselho da Europa, 1950).

Outra ilustração é a Carta dos Direitos Fundamentais da União Europeia, que consagra, em termos amplos, o direito dos indivíduos à salvaguarda da sua privacidade e à proteção dos seus dados pessoais. A Carta, no seu art.º 7º, garante o direito "ao respeito pela vida sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações", bem como, no nr.º 1 do art.º 8º, o direito à proteção dos dados pessoais que digam respeito às pessoas, além disso, a Carta afirma no nr.º 2 do mesmo artigo, que os dados pessoais devem ser tratados de forma leal, "para fins específicos" consentidos pelo interessado/a ou com fundamentação legal, e ainda, que todos os cidadãos podem consultar os dados que foram recolhidos, e ainda têm direito à obtenção da respetiva retificação (UE, 2000).

Na garantia dos direitos suprarreferidos, têm sido implementadas medidas que procuram proteger os dados pessoais, assim, entrou em vigor a 25 de maio de 2018 o Regulamento Geral de Proteção de Dados, Regulamento UE n.º 2016/679, que vem definir o tratamento de dados pessoais e da livre circulação dos mesmos, de forma a uniformizar os diversos sistemas nacionais (UE, 2016).

As regras para o processamento de dados pessoais de indivíduos na UE são estabelecidas pelo RGPD, que impõe novos procedimentos tecnológicos para reforçar a proteção legal dos direitos dos titulares de dados por parte de indivíduos, empresas ou organizações (Albuquerque, 2022).

Tratando-se do desenvolvimento tecnológico dos sistemas de videovigilância, torna-se então indispensável mencionar a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, sendo fundamental no âmbito da videovigilância policial, pois estabelece as regras para o processamento de informações pessoais pelas autoridades competentes no âmbito da "prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais" (EU, 2016, p. 89), bem como a "livre circulação desses dados" (EU, 2016, p. 89),

essa diretiva revoga a Decisão-Quadro 2008/977/JAI do Conselho "no domínio da cooperação judiciária em matéria penal e da cooperação policial" (UE, 2016, p. 89).

A Diretiva 2016/680 da UE estabelece a proteção de dados pessoais no contexto da aplicação da lei, define regras para o processamento de dados pessoais pelas autoridades competentes pela aplicação da lei nos Estados membros da EU, tendo como objetivo proteger os direitos fundamentais das pessoas, em particular o direito à privacidade, e garantir que o processamento de dados pessoais pelas autoridades responsáveis pela aplicação da lei seja realizado de forma justa, transparente e legal. A mesma se estende a todas as atividades de tratamento de informações pessoais conduzidas pelas autoridades encarregadas da aplicação da lei no âmbito da prevenção, investigação, deteção ou repressão de crimes ou infrações penais (UE, 2016; Hert & Papakonstantinou, 2011).

Entre outras coisas, a diretiva estabelece regras sobre a recolha, armazenamento, uso, divulgação e exclusão de dados pessoais pelas autoridades responsáveis pela aplicação da Lei. Exige também que as autoridades nomeiem um encarregado de proteção de dados, realizem avaliações de impacto à proteção de dados quando necessário, e estabeleçam medidas adequadas de segurança para proteger os dados pessoais que elas processam (UE, 2016).

Ainda no contexto da videovigilância, é importante referir a utilização da IA. Neste contexto, a Comissão Europeia (CE) (2020) emite o *Livro Branco sobre a inteligência artificial: uma abordagem europeia virada para a excelência e a confiança*, sendo um documento estratégico que apresenta as políticas e iniciativas propostas pela UE para promover a inovação e a utilização responsável da IA na Europa, respeitando os DLG dos cidadãos, diretos estes previstos constitucionalmente.

Consequentemente, com o objetivo de preservar a liderança tecnológica da UE e garantir que as novas tecnologias sejam desenvolvidas em conformidade com os valores, direitos e princípios da mesma, o Parlamento Europeu (PE) elabora, no mesmo ano, a Proposta de Regulamento do Parlamento Europeu e do Conselho 2021/006 (COD). Nesse sentido, a Comissão Europeia procura estabelecer regras harmonizadas para a IA, pretendendo alterar atos legislativos, de modo a assegurar que a IA esteja ao serviço dos cidadãos (CE, 2020)

1.4. Direito Nacional

Neste subcapítulo serão analisados os diplomas legais portugueses que devem ser tidos em consideração quanto à utilização de sistemas de videovigilância policial em espaços públicos.

Assim como previsto na DUDH e na CEDH, também a Constituição da República Portuguesa (CRP) protege os direitos relacionados com a proteção dos dados pessoais e da imagem, conforme os arts.º 26º *Outros direitos pessoais* e 35.º *Utilização da informática*. (AR, 1976). Ainda é de referir o art.º 80.º do Código Civil, aprovado pelo Decreto-Lei n.º 47344/66, de 25 de novembro, *direito à reserva sobre a intimidade da vida privada*, que no seu n.º 1 "todos devem guardar reserva quanto à intimidade da vida privada de outrem." (Governo, 1966, p. 70).

Refere Moleirinho (2021, p. 6) que a recolha, processamento e partilha de dados pessoais no âmbito da atividade policial, de forma geral, e na investigação criminal, em específico, tem vindo a ser amplamente discutidos do ponto de vista "jurídico, operacional e social".

Conforme anteriormente visto, a UE, através da Diretiva 95/46 CE revogada pelo Regulamento da UE 2016/679 de 27 de abril, RGPD, determina as limitações referentes ao uso e tratamento de dados pessoais, assim a Assembleia da República portuguesa, através da Lei n.º 58/2019, de 8 de agosto, assegura a execução desse regulamento, relativo "à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados" (AR, 2019a, p. 3), transpondo assim para o nível nacional o RGPD. Ainda é de referir a Lei n.º 59/2019, de 8 de agosto, que transpôs a Diretiva (UE) 2019/680, esta no âmbito dos "dados pessoais para prevenção, deteção, investigação ou repressão de infrações penais" (AR, 2019b, p. 41).

No que diz respeito à legislação nacional referente à videovigilância policial, foi primeiramente a Lei n.º 1/2005, de 10 de janeiro, que regulou a sua utilização, com as respetivas alterações implementadas pela Lei n.º 39-A/2005, de 29 de julho, pela Lei n.º 53-A/2006, de 29 de dezembro, posteriormente pela Lei n.º 9/2012, de 23 de fevereiro, e por fim revogada pela Lei n.º 95/2021, de 29 de dezembro (AR, 2021).

Pode-se dizer então que os sistemas de videovigilância policial, em Portugal, são regulados pela Lei n.º 95/2021, de 29 de dezembro, com as Portarias n.º 372/2012 e n.º 373/2012, ambas de 16 de dezembro, estas regulam tanto "os requisitos técnicos mínimos das câmaras fixas e portáteis de videovigilância", como "aprova o modelo de avisos e

simbologia da utilização de câmaras de vídeo pelas forças e serviços de segurança em locais públicos de utilização comum", respetivamente (AR, 2012). Não obstante, importa realçar a necessária conjugação com a legislação que regula o tratamento de dados pessoais, nomeadamente as Leis n.º 58/2019 e 59/2019, ambas de 8 de agosto.

Importa então saber o objeto em questão que se pretende regular, conforme o art.º 1º da Lei 95/2021, de 29 de dezembro, "a presente lei regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC) a sistemas de videovigilância, para captação, gravação e tratamento de imagem e som." (AR, 2021, p. 3), e a mesma aplica-se segundo o art.º 2º, aos "sistemas de videovigilância instalados ou utilizados no espaço público ou nos espaços privados de acesso público, quando devidamente autorizados para os fins previstos no artigo seguinte" (AR, 2021, p. 3). No art.º 3º da mesma Lei *Fins dos sistemas,* e em conjugação com a Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto, vem limitar, de forma taxativa, os fins para os quais os sistemas podem ser utilizados, por exemplo na alínea c) do n.º 1 refere que pode ser utilizado para "proteção da segurança das pessoas, animais e bens, em locais públicos ou de acesso público, e a prevenção da prática de factos qualificados pela lei como crimes, em locais em que exista razoável risco da sua ocorrência" (AR, 2021, p. 3), ou na alínea g) do mesmo n.º "controlo de tráfego e segurança de pessoas, animais e bens na circulação rodoviária" (AR, 2021, p. 3).

É importante destacar que, de acordo com a Lei n.º 95/2021, de 29 de dezembro, e em conformidade com o RGPD, há disposições relacionadas à captura de imagens, recolha e tratamento de dados. O art.º 16º prevê que o tratamento de dados pode ser fundamentado em critérios técnicos, desde que estejam alinhados com os objetivos do sistema em questão. No entanto, é importante notar que a captação e tratamento de dados biométricos, conhecido como reconhecimento facial, é proibido. Por sua vez, o art.º 17º estabelece que a competência para o tratamento de imagens e sons é da Forças e Serviços de Segurança (FFSS) requerentes, ou da ANEPC, com competência na área em que é recolhida a imagem. Este tratamento está sujeito à Lei n.º 59/2019, de 8 de agosto, e aplica-se a todos os contratos celebrados com terceiros (AR, 2021).

É fundamental que sejam tomadas medidas rigorosas para garantir a proteção de dados sensíveis, como os biométricos, e que sejam respeitados os procedimentos legais de tratamento de dados. Além disso, a atribuição clara de responsabilidade é necessária no tratamento de imagens e sons, independentemente da entidade que esteja envolvida, para que

sejam evitados potenciais abusos ou violações dos direitos dos cidadãos (Pessoa, entrevista, 21.04.2023).

É também necessário referir os pareceres emitidos pela Comissão Nacional de Proteção de Dados (CNPD) 30/2012 e 58/2012, de 17 de maio e de 2 de outubro respetivamente, mesmo que não façam parte do ordenamento jurídico, os mesmo foram devidamente considerados na formulação da Portaria n.º 372/2012, anteriormente referida (AR, 2012).

CAPÍTULO 2 – APLICAÇÕES TECNOLÓGICAS DOS SISTEMAS DE VIDEOVIGILÂNCIA POLICIAL

2.1. Evolução dos sistemas de videovigilância

A sociedade e a tecnologia estão em constante evolução e desenvolvimento, e é importante acompanhar essa evolução para garantir que as tecnologias sejam usadas de forma benéfica para a sociedade. Com o passar do tempo, houve uma necessidade crescente de aprimorar as técnicas de vigilância, a fim de aproveitar o avanço da tecnologia e das telecomunicações, a fim de obter melhores resultados. Como resultado, a videovigilância passou por várias gerações, cada uma com suas próprias características tecnológicas e funcionalidades, a evolução dos sistemas de vigilância inteligente pode ser categorizada em três gerações distintas. A primeira geração utilizava técnicas analógicas, enquanto a segunda passou por uma mudança das abordagens analógicas para as digitais. Atualmente, na terceira geração, é utilizado o processamento digital de vídeo e outras interfaces, juntamente com a adição de recursos de tomada de decisão e alerta ao sistema. (Arroyo et al., 2015; Durães, 2008).

Referem Durães (2008) e Bruno (2012) que a **primeira** geração dos sistemas de videovigilância começou pelas *Close Circuit Television* (CCTV). Nesta geração os sistemas eram analógicos e consistiam em câmaras conectadas a um monitor por meio de cabos coaxiais. Múltiplas câmaras são ligadas a um monitor usando um *switch*, e o monitor é normalmente instalado numa sala de controlo, a qual é supervisionada por uma ou mais pessoas. A captura imagens era realizada de maneira digital e, posteriormente, convertida em sinal analógico. Esses sistemas focavam-se na pesquisa sobre tecnologias analógicas versus digitais, gravação digital e compressão de vídeo. Essa conversão, no entanto, pode causar uma degradação significativa na qualidade da imagem, pois o sinal analógico é mais

suscetível ao ruído. Na época, o desenvolvimento desses sistemas concentrou-se na pesquisa sobre tecnologias analógicas versus digitais, gravação digital e compressão de vídeo.

Na **segunda** geração, os sistemas de videovigilância são digitais e utilizam tecnologia de rede IP (*Internet Protocol*). As câmaras são conectadas à rede e as imagens são transmitidas em formato digital, o que reduz a perda de qualidade. Esses sistemas também permitem o armazenamento e o gestão centralizado de grandes quantidades de dados de vídeo. Esta geração de sistemas de videovigilância é caracterizada por uma evolução dos sistemas analógicos para sistemas digitais, com a introdução da referida tecnologia IP e algoritmos de análise de comportamentos. Esses sistemas semiautomáticos são capazes de detetar objetos, pessoas e analisar seus comportamentos em tempo real. (Durães, 2008, Bruno, 2012).

Embora a **segunda** geração tenha melhorado a eficiência dos sistemas de videovigilância em comparação com a primeira geração, esta também apresenta desafios em relação à robustez dos algoritmos de deteção e análise de comportamento. A qualidade das imagens, a iluminação, a presença de obstáculos e outras variáveis podem afetar a precisão dos algoritmos, tornando necessário o desenvolvimento contínuo de técnicas mais avançadas para melhorar a sua robustez (Durães, 2008).

Segundo Arroyo et al. (2015) os sistemas de videovigilância da **terceira** geração são sistemas avançados que combinam tecnologia de vídeo inteligente, análise de dados e aprendizagem de máquina para fornecer recursos mais sofisticados. Esses sistemas são capazes de detetar e alertar sobre atividades suspeitas em tempo real, além de realizar análises de comportamento para prever possíveis ameaças. Efetivamente também permitem a integração com outras tecnologias, como reconhecimento facial e sensores de movimento.

A **terceira** geração de sistemas de videovigilância atingiu um certo grau de automatização que permite detetar comportamentos humanos suspeitos e emitir os alarmes correspondentes. Cumpre referir que, "a terceira geração tem como objetivo desenvolver tecnologias de compreensão automática de vídeo, permitindo a um único operador humano controlar comportamentos humanos nas mais complexas áreas civis" (Durães, 2008, p. 5). Durães (2008) ainda refere que na maioria dos casos, esses sistemas seguem um padrão semelhante para definir sua metodologia de atuação com base em várias etapas sequenciais, que consistem principalmente na deteção de objetos em primeiro plano, monitoramento e análise comportamental.

Atualmente, as pesquisas nesta área estão focadas na fusão de dados, na comparação entre a abordagem centrada na inteligência versus a abordagem distribuída e nas técnicas de

vigilância que envolvem múltiplas câmaras. À medida que nos dirigimos para o futuro, é prevista uma melhoria no processamento de imagem, permitindo que os sistemas desempenhem tarefas de maior complexidade. Outros campos de investigação englobam o fortalecimento dos algoritmos de deteção, reconhecimento de objetos, seguimento e reconhecimento de comportamentos humanos, bem como a criação de soluções inovadoras para a comunicação em sistemas de vigilância distribuídos (Durães, 2008; Arroyo et al., 2015).

Em suma, a videovigilância evoluiu ao longo do tempo, desde a era analógica até a era da IA. Cada geração trouxe novas funcionalidades e melhorias na qualidade e capacidade de vigilância tornando estes sistemas cada vez mais proficientes. No subcapítulo "Inteligência artificial nos sistemas de videovigilância" serão explicadas algumas das técnicas aplicadas nos sistemas de videovigilância.

2.2. Videovigilância policial em espaços públicos

A realidade policial tem se alterado, existindo novos desafios, cada vez mais complexos, no âmbito da segurança. Assim torna-se necessário aumentar a eficácia operacional das várias FFSS, pelo que, para se obter a pretendida segurança e tranquilidade públicas, têm sido implementados diversos sistemas e ferramentas tecnológicas. Neste sentido, os sistemas de videovigilância policial em espaços públicos têm se destacado devido à sua importância na proteção de pessoas e bens, especialmente em áreas com altos índices de criminalidade. As vantagens desses sistemas são amplamente reconhecidas, já que eles ajudam a prevenir crimes, fornecem evidências para investigações criminais e permitem uma resposta mais rápida a emergências (Albuquerque, 2022).

A tecnologia moderna de câmaras de vigilância, em constante evolução, oferece um potencial cada vez maior para a recolha e uso de imagens e informações associadas. Esses avanços aumentam consideravelmente a capacidade de capturar, armazenar, partilhar e analisar imagens e dados. Esta tecnologia pode ser uma ferramenta valiosa na gestão da segurança pública e na proteção de pessoas e bens, na prevenção e investigação criminal, e na aplicação da justiça pelos tribunais. Os avanços tecnológicos também podem oferecer maior oportunidade de proteção da vida privacidade. Utilizada de forma adequada, a tecnologia atual e futura pode fornecer uma solução proporcional e eficaz quando a videovigilância visa um objetivo legítimo e atende a uma necessidade premente (Police Transparency Unit, 2013).

Para se entender a videovigilância policial, é necessário primeiramente conceptualizar a videovigilância. Assim, diz a Porto Editora (2023), que a videovigilância consiste em "vigilância feita com recurso a sistemas de vídeo (câmaras de filmar, sistemas de deteção automática de movimento, etc.)", refere ainda Pereira (2017) que a videovigilância consiste na gravação de imagens e áudio utilizando um suporte magnético, que são visualizados num monitor. A videovigilância envolve a utilização de um sistema de monitorização, que utiliza câmaras de vídeo para capturar imagens num local específico, seja ele dentro ou fora, durante um período de tempo determinado ou não. Geralmente, essas câmaras possuem software conectado à Internet, permitindo que as imagens sejam transmitidas e visualizadas em tempo real. Assim podemos dizer que a videovigilância é um sistema de segurança que utiliza câmaras de vídeo, com o objetivo de proteger e controlar o acesso através da monitorização e gravação de imagens, incluindo ou não sons, de um determinado espaço, seja ele interior ou exterior. As imagens capturadas pelas câmaras podem ser visualizadas em tempo real e/ou gravadas para posterior análise e investigação. A videovigilância pode ser utilizada tanto para fins de segurança pública, com o objetivo de prevenir e combater a criminalidade, identificar suspeitos ou gerir emergências. (Nunes, 2011)

Percebendo o que é a videovigilância, e transpondo esse conceito para a realidade policial, a videovigilância policial é um sistema de monitorização que utiliza câmaras de vídeo para ajudar as FFSS a monitorizar e prevenir crimes em áreas públicas. Estas câmaras de vigilância são colocadas em locais estratégicos e monitorizam atividades suspeitas ou ilegais, transmitindo as imagens para uma central. O objetivo da videovigilância policial é aumentar a segurança pública e ajudar a prevenir atividades criminosas, tais como assaltos, roubos, vandalismo, tráfico de drogas, entre outros. Ademais, as imagens capturadas pelas câmaras de vigilância podem ser usadas para investigações criminais e fornecer provas em processos judiciais. No entanto, a videovigilância policial é frequentemente alvo de críticas e preocupações sobre a privacidade, liberdade e potencial abuso de poder por parte das autoridades, apresentando desse modo diversos desafios na sua aplicação em espaço público. Assim, e como referido anteriormente, foi necessário regular a utilização de sistemas de videovigilância policial (Nunes, 2011; Pereira, 2017).

Tendo já sido feito, no capítulo anterior, o enquadramento da Lei n.º 95/2021, de 29 de dezembro, aqui será exposto alguns dos artigos fundamentais para a compreensão do conceito de videovigilância policial. Começando pelo objeto da referida lei, que no seu art.º 1º refere que a mesma regula a "utilização e o acesso pelas forças e serviços de segurança e

pela Autoridade Nacional de Emergência e Proteção Civil (ANEPC) a sistemas de videovigilância" (AR, 2021, p 3). No entanto, conforme o seu art.º 2º n.º1 da referente Lei, aplica-se aos sistemas de videovigilância "quando devidamente autorizados para os fins previstos" (AR, 2021, p 3). No art. º 3º da mesma, *Fins dos sistemas,* refere que a utilização de sistemas de videovigilância em espaços públicos está também regulamentada pela Lei de Segurança Interna, aprovada pela Lei n.º 53/2008, de 29 de agosto. De acordo com essa lei, os sistemas de videovigilância têm a finalidade de proteger edifícios e infraestruturas públicas, infraestruturas críticas e pontos sensíveis, bem como apoiar as operações policiais complexas e prevenir a prática de crimes em locais de risco. Além disso, esses sistemas também são empregues na prevenção de atos terroristas, resposta a incidentes de segurança em andamento e controlo de tráfego rodoviário, entre outras finalidades mencionadas na lei. A Lei de Segurança Interna prevê que a instalação de sistemas videovigilância nas instalações policiais de atendimento ao público é permitida (AR, 2021; AR, 2008).

Como refere o mesmo diploma, a instalação dos sistemas de videovigilância por parte das FFSS está dependente de autorização do membro do governo que exerce tutela sobre a "força ou serviço de segurança requerente ou a ANEPC" (AR, 2021, p. 3). Assim, Albuquerque (2022, p. 16) resume os elementos do pedido de autorização para instalação de sistemas de videovigilância, referindo o art.º 6º da Lei n.º 95/2021, de 29 de dezembro, e também o art.º 29º da Lei n.º 59/2019, de 8 da agosto, elaborando o seguinte quadro:

Tabela 1 - Elementos do pedido de autorização para instalação de sistemas de videovigilância

Diploma	Elementos
Lei n.º 95/2021, de 29 de dezembro (Art.º 6º)	- Fundamentação da necessidade; - Identificação do local e área abrangidos pela captação e dos pontos de instalação das câmaras; - Características técnicas do equipamento; - Identificação da FS responsável pela conservação e tratamento dos dados; - Procedimentos de informação ao público sobre a existência do sistema; - Descrição dos critérios utilizados no sistema de gestão analítica dos dados captados; - Mecanismos tendentes a assegurar o correto uso dos dados registados; - Avaliação de impacto do tratamento de dados sobre a proteção de dados pessoais.
Lei n.º 59/2019, de 8 da agosto (Art.º 29º)	(Avaliação do Impacto) - Descrição geral das operações de tratamento previstas; - Avaliação dos riscos para os DLG dos titulares dos dados;

	- Medidas previstas mitigar os riscos; - Garantias, medidas de segurança e mecanismos para assegurar a proteção de dados pessoais e demonstrar a conformidade do tratamento

Fontes: Albuquerque, 2022, p. 16; Lei n.º 95/2021, de 29 de dezembro, e Lei n.º 59/2019, de 8 de agosto

O dirigente máximo da FFSS, ou da ANEPC, deve apresentar o pedido de autorização para instalar sistemas de videovigilância, o qual deve ser acompanhado pelos elementos descritos no quadro anterior. A decisão da autorização para a instalação dos sistemas é ainda precedida do parecer da CNPD, esta o avalia o cumprimento das normas relativas à segurança no tratamento dos dados recolhidos e ainda analisar o que diz respeito aos n.º 4 a 6 do art.º 4º e aos art.º 16º, 18º a 20º e 22º, conforme o disposto na Lei 95/2021. (AR, 2021).

2.3.Aplicabilidade dos sistemas de videovigilância policiais

Neste subcapítulo é analisada a aplicabilidade os sistemas de videovigilância policiais. Conforme refere o Relatório Anual de Segurança Interna (RASI) relativo ao ano 2022, o terceiro objetivo estratégico para 2023, é a implementação de sistemas de tecnologia compartilhada pelas Forças de Segurança do MAI, especificamente em relação à videovigilância (Sistema de Segurança Interna [SSI], 2023, p. 162).

2.3.1. Videovigilância policial na prevenção

Uma das premissas da videovigilância será a prevenção de ilícitos criminais. Cusson e Lemieux (2007, p. 404) afirmam que, a prevenção criminal abrange todas as medidas não coercivas relacionadas às causas, motivos e fatores preliminares da criminalidade, com o objetivo de diminuir a probabilidade da sua ocorrência ou da sua gravidade.

O art.º 1º da Lei de Organização da Investigação Criminal, aprovada pela Lei nº 49/2008 de 27 de agosto, define a investigação criminal como o "conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher as provas, no âmbito do processo" (AR, 2008, p. 2).

Na perspetiva de proteção dos direitos individuais contra possíveis abusos no exercício dessa atividade, Monte (2013, p. 91) afirma que o atual sistema penal é uma conquista importante da humanidade, uma vez que conferiu aos indivíduos um estatuto de destaque, garantindo-lhes proteção penal, especialmente contra abusos do Estado. De maneira geral, entende-se que a função do policiamento preventivo é antecipar comportamentos desviantes que possam apresentar riscos, chegando, em última instância, a ter caráter criminoso.

Como refere Moleirinho (2018), com o objetivo de prevenir a ocorrência de crimes, têm sido adotadas e aprimoradas diversas estratégias de policiamento proativo e de aproximação comunitária, visando a coprodução de segurança e a identificação de situações de risco. Tais metodologias têm se mostrado efetivas para a prevenção de delitos, na medida em que estimulam a participação ativa da comunidade no processo de segurança pública e permitem uma abordagem mais abrangente e integrada do fenómeno criminal. Além disso, a adoção dessas estratégias pode contribuir para a construção de uma relação de confiança e de diálogo entre a polícia e a sociedade, o que pode ser benéfico tanto para a prevenção quanto para a resolução de casos criminais.

Importa ainda referir que esta tipologia de policiamento proativo e de aproximação comunitária demanda um planeamento de longo prazo, em que a polícia procura identificar e atuar sobre as causas subjacentes ao crime, em vez de simplesmente reagir a incidentes e denúncias. Enquanto o policiamento reativo tem como foco principal a resposta a eventos já ocorridos, o policiamento proativo procura antecipar e prevenir esses eventos, por meio da análise de dados criminais, da identificação de áreas de risco e da promoção de intervenções preventivas e de segurança comunitária. Dessa forma, o policiamento proativo tende a ser mais estratégico e a demandar uma visão de longo prazo por parte da polícia, em vez de uma abordagem meramente reativa (Moleirinho, 2021).

Neste sentido a videovigilância atua na prevenção, sendo uma ferramenta cada vez mais utilizada no policiamento proativo e preventivo, permitindo vigiar áreas específicas em tempo real e identificar atividades suspeitas antes que os crimes ocorram. Ao instalar câmaras em locais estratégicos, a videovigilância permite que a força policial supervisionar de forma eficaz as atividades suspeitas, identificando comportamentos criminosos antes que se tornem uma ameaça para a segurança pública. Além disso, a videovigilância também pode ajudar a recolher provas em caso de crimes já ocorridos, facilitando a identificação e punição dos responsáveis.

A videovigilância também pode ser utilizada em conjunto com outras tecnologias, como reconhecimento facial ou a analítica de vídeo, para identificar pessoas ou comportamentos suspeitos e prevenir ações criminosas.

2.3.2. Analítica de vídeo

A Analítica de vídeo, conhecida tambem como “Análise Inteligente de Vídeo”, é uma tecnologia capaz de analisar imagens de vídeo automaticamente para detetar e identificar eventos e objetos. Essa solução é baseada em IA e Visão Computacional, onde as câmaras

funcionam como "olhos" do sistema de vídeo analítico e este, por sua vez, é como um "cérebro" que interpreta o que está a ser visualizado. Essa tecnologia proporciona uma ampla gama de aplicações, desde a identificação de elementos concretos, até ao seguimento desses elementos na imagem (Segurança Eletrônica, 2022). A habilidade de analisar as informações em vídeo das câmaras e tomar decisões ou emitir alertas com base nos resultados obtidos torna as operações de segurança e mais eficientes de forma imediata (Security Magazine, 2021). Aliado a isso, é ainda utilizada a deteção de movimento que emite um alerta aos operadores e ativa a gravação de vídeo quando o movimento é detetado em uma cena que, de outra forma, seria estática, o que também melhora significativamente a eficiência da videovigilância.

A deteção de movimento, o reconhecimento facial, a contagem de pessoas e o reconhecimento de matrículas de veículos, é possível com a utilização da analítica de vídeo, é possível aumentar a eficiência de sistemas de segurança e vigilância, permitindo que os operadores sejam alertados de forma automática quando alguma atividade suspeita é detetada, essa análise é realizada através de um algoritmo que passa por um processo de treino para reconhecer imagens específicas (Segurança Eletrónica, 2022).

Entre diversas modalidades de funcionamento, a Segurança Eletrónica (2022) aponta as principais e mais utilizadas, que são as seguintes:

Deteção de elementos específicos, o que marca realmente a utilização da analítica de vídeo é a capacidade de "identificação de elementos específicos na imagem, ou seja, ao ensinar ao sistema como um corpo humano se parece, por exemplo, sempre que uma pessoa aparecer nos registros de vídeo, o algoritmo saberá identificá-la" (Segurança Eletrónica, 2022), assim é possível diferenciar uma pessoa de um carro e de animal, assim no caso dos sensores de movimento a fim de detetar intrusões, o sistema consegue entender se é apenas um animal ou a até mesmo a vegetação movida com o vento, então o sistema foca-se apenas nos elementos desejados, sendo assim mais assertivo e eficiente.

Cruzamento de Linha Virtual, com essa tecnologia, é possível criar linhas virtuais em locais decisivos para monitorizar sempre que algum elemento cruze essas linhas. Desse modo, podemos estabelecer barreiras virtuais em muros ou entradas, por exemplo, que emitirão um aviso sempre que alguém as atravessar (ver figura 1):

Figura 1 - Linha Virtual

Fonte – Segurança Eletrónica (2022)

ROI: Region Of Interest (região/área de interesse) como alternativa a controlar todas as áreas exibidas no vídeo, o que pode exigir muito processamento do sistema, assim como a criação da linha virtual, além disso, é possível direcionar a deteção para alvos específicos em regiões específicas. Por exemplo, se estiver a ser monitorizada a entrada de um parque de estacionamento onde apenas a entrada de veículos é permitida e a passagem de pessoas é proibida, pode ser ciado uma *ROI* para detetar pessoas na entrada do parque. Dessa forma, quem entrar na área de interesse será detetado, enquanto os veículos serão desconsiderados, tornando o controle mais prático e eficiente (ver figura 2)

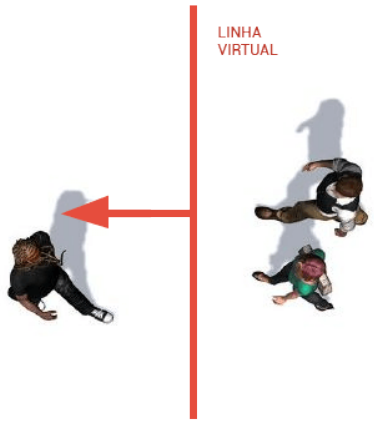
Figura 2 - Region of Interest

Fonte: Segurança Eletrónica (2022)

Sentido do Movimento, outra capacidade da análise de vídeo que é apontada pela Segurança Eletrónica (2022), é o sentido de movimento que tem a capacidade de identificar o sentido em que determinado elemento se move, o que pode ser utilizado em conjunto com o *Cruzamento de Linha Virtual* para determinar se o elemento está a entrar ou a sair de uma área específica. Em estabelecimentos comerciais que possuem uma mesma porta de entrada

e saída, por exemplo, é possível configurar o sistema para detetar somente as pessoas que entram e ignorar as que saem, escolhendo a direção correta do movimento (ver figura 3).

Figura 3 - Sentido de movimento



Fonte: Segurança Eletrónica (2022)

Reconhecimento de Comportamentos, a analítica de vídeo não se limita apenas à deteção de pessoas, mas também pode ser usado para identificar comportamentos específicos. Por exemplo, essa função pode ser empregue para controlar indivíduos que que rondam um determinado local, que estejam a correr ou que estejam envolvidos em rixas.

Por último, a Segurança Eletrónica (2022) refere a *Contagem de Elementos,* as áreas de *Marketing e Business Intelligence,* utilizam bastante esta função, no entanto também é aplicável em outras áreas, como na segurança. A contagem de pessoas em determinada área, por exemplo, é uma informação crucial para a força policial e difícil de ser calculada. E ainda, é possível calcular o período que cada indivíduo/objeto esteve na área controlada (Segurança Eletrónica, 2022).

2.3.3. Videovigilância florestal

Além da utilidade que os sistemas de videovigilância têm no combate à criminalidade, estes sistemas também demonstram sua aplicabilidade no que concerne à proteção das florestas. Essa vertente da utilização da videovigilância permite a deteção antecipada e precisa de ignições, possibilitando uma resposta mais rápida e efetiva no combate a incêndios florestais. Os sistemas de videovigilância baseados em tecnologias avançadas, como a IA, e a analítica de vídeo, podem controlar extensas áreas florestais em tempo real. Eles identificam com precisão focos de incêndio em estágios iniciais, permitindo que as autoridades sejam alertadas imediatamente. Isso possibilita a mobilização rápida de meio de combate a incêndios, contribuindo para a minimização dos danos causados aos

ecossistemas florestais e à fauna local. Além disso, o registo contínuo de imagens proporcionado pelos sistemas de videovigilância pode ajudar na identificação de atividades humanas suspeitas, como desmatamento ilegal ou comportamento criminoso, promovendo ações preventivas e preservando a biodiversidade das florestas (GNR, 2022)

Conforme refere Alves (2018), as tecnologias de deteção mais utilizadas são: as câmaras de luz visível, com energia solar e deteção de fumo que requerem monitorização visual constante, causando fadiga e perda de concentração nos operadores; câmaras a preto e branco, que utilizam diferenças de contraste para deteção de fumo, enquanto câmaras coloridas comparam imagens consecutivas para identificar variações de cor, no entanto as vibrações e movimentos das câmaras dificultam a deteção automática, essa tecnologia apresenta limitações, como a incapacidade de detetar fumo à noite e dificuldade em distinguir fumo de nuvens, poeira e baixa luminosidade; câmaras com sensores térmicos, estas detetam a energia irradiada pelo fogo sem fonte externa, porém perdem eficácia em temperaturas semelhantes ao ambiente, podem operar durante o dia e à noite, com processamento de imagens mais simples e tempo de deteção reduzido; a espectroscopia ótica com espetrômetro permite a deteção automática de elementos de fumo na atmosfera, sem intervenção humana, essa tecnologia possui grandes limitações durante a noite, pois só consegue identificar fumo após atingir a linha do horizonte, resultando em atrasos para uma resposta inicial eficaz (COTEC/ADAI, 2005; Alves, 2018).

CAPÍTULO 3 – INTELIGÊNCIA ARTIFICIAL NOS SISTEMAS DE VIDEOVIGILÂNCIA

3.1. Introdução

Na senda de entender os conceitos inerentes ao tema, surge a IA. Como tal, neste capítulo, será explorado o papel da IA na videovigilância e a sua interação com a proteção de dados pessoais. Serão ainda abordado os benefícios e os desafios dessa tecnologia, bem como as medidas necessárias para garantir a segurança e a privacidade das informações retidas.

Existe uma crescente utilização da IA, como referem Kissinger, Schmidt e Huttenlocher (2021, p. 21) “embora o avanço da IA possa ser inevitável, o seu destino final não o é”, e ainda acrescentam que a IA é “um veículo de muitos ramos de atividade e facetas

da vida humana: investigação científica, educação, manufatura, logística, transportes, defesa, justiça, publicidade, arte, cultura e mais" (Kissinger, et al. 2021, p. 10).

Em geral, qualquer aumento na capacidade da tecnologia de sistemas de videovigilância, tem o potencial de aumentar a probabilidade de invasão da privacidade de um indivíduo. Conforme a tecnologia de vigilância evolui e se torna mais avançada e capacitada para de capturar, armazenar e analisar grandes quantidades de informações, incluindo imagens da vida privada, surge a preocupação de que a privacidade das pessoas possa ser comprometida. É importante encontrar um equilíbrio entre o uso dessas tecnologias para finalidades legítimas, como garantir a segurança pública e resguardar os direitos individuais, especialmente o direito à privacidade (Police Transparency Unit, 2013).

3.2. Inteligência artificial

Existem muitos medos relacionados à IA, sendo baseados em conceitos hipotéticos, como IA geral, superinteligência artificial e singularidade, que teoricamente poderiam levar a uma mudança de poder dos humanos para a IA e criar máquinas que poderiam até mesmo libertar-se do controlo humano. No entanto, ressalva que há dúvidas significativas quanto à possibilidade de alcançar essa IA especulativa com as nossas tecnologias e leis científicas (PE, 2021b).

Segue-se a definição de IA adotada pelo PE, que se refere à "capacidade que uma máquina para reproduzir competências semelhantes às humanas como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade" (PE, 2021a).

Ainda preconizado pela UE no Livro Branco sobre a inteligência artificial: "a IA é um conjunto de tecnologias que combinam dados, algoritmos e capacidade computacional. Os progressos em computação e a cada vez maior disponibilidade de dados são, por conseguinte, os principais motores do atual impulso da IA." (CE, 2020, p. 2). Em complemento, referido pela UE (2018) "O conceito de inteligência artificial (IA) aplica-se a sistemas que apresentam um comportamento inteligente, analisando o seu ambiente e tomando medidas — com um determinado nível de autonomia — para atingir objetivos específicos." (CE, 2018, p. 1).

Para entender o conceito de IA, é necessário também conhecer-se os conceitos que lhes são subadjacentes, como *Dados*, *Algoritmos*, *Big Data*, *Aprendizagem de Máquina* e *Aprendizagem Profunda*.

Começando com o conceito de *Dados*, importa ressalvar o estabelecido no art.º 3º, n.º1, al. c) e o), do Regulamento de tratamento de dados pessoais, aprovado pela Lei n.º 59/

2019, de 8 de agosto, que define "«Dados pessoais», como informações relativas a uma pessoa singular identificada ou identificável" (AR, 2019b, p. 3), e "«Dados biométricos», dados pessoais resultantes de um tratamento técnico específico, relativos às características físicas, fisiológicas ou comportamentais de uma pessoa singular, que permitam ou confirmem a sua identificação única, tais como imagens faciais ou dados dactiloscópicos" (AR, 2019b, p. 3).

No que diz respeito a *Algoritmos*, trata-se de uma sequência de instruções que orienta um computador sobre o que fazer. Os algoritmos evolutivos também são capazes de realizar algo mais subtil como conectar pontos entre eventos que, de forma isolada, parecem inofensivos, mas que, em conjunto, mostram uma ameaça latente (Domingos, 2017).

Relativamente ao conceito de *Big Data*, refere (Costa, 2021) e Domingos (2012) que o conceito é amplo e pode-se referir a conjuntos de dados de grande escala, provenientes de diversas fontes e em diferentes formatos. Também engloba as tecnologias e processos necessários para recolher, armazenar e analisar esses dados, transformando-os um conhecimento específico. Os dados brutos, como imagens, vídeos, textos ou sons, não possuem valor intrínseco, mas podem ser lapidados por algoritmos que os analisam e interpretam. A mineração de dados é especialmente importante para descobrir padrões e correlações entre grandes conjuntos de dados, convertendo-os em informações valiosas que podem ser transformadas em ativos valiosos. Em resumo, o *big data* é um termo que abrange tanto a quantidade de dados quanto as tecnologias e processos para gerenciá-los e extrair informações úteis.

No campo da IA é ainda importante referir tanto a *Aprendizagem de Máquina* como a *Aprendizagem Profunda*. Domingos (2017) clarifica e distingue ambos. A primeira assume diversas formas e é conhecida por muitos nomes diferentes, como identificação de padrões, análise estatística, extração de informações, descoberta de insights, previsão de tendências, análise de dados avançada, sistemas adaptativos, sistemas autônomos, técnicas de aprendizado de máquina (Domingos, 2017), tecnicamente, a aprendizagem de máquina é um subcampo da IA. A aprendizagem de máquina é como ter um radar que prevê eventos futuros, não podemos simplesmente responder às ações do adversário, devemos prever e evitar as suas manobras. Quanto que a segunda, é uma das áreas mais recentes da IA, cujos algoritmos são baseados em dados gerados pelas interações de múltiplas camadas de aprendizagem de máquina. A grande quantidade de dados digitais disponíveis para alimentar esses sistemas de aprendizagem, juntamente com melhorias nas ferramentas para

processamento de dados, o uso de software de código aberto e a disponibilidade de infraestrutura de nuvem acessível, levaram a uma explosão de inovação na IA moderna.

Algoritmos são procedimentos informatizados que resolvem problemas ou atingem objetivos, transformando dados de entrada em resultados. A análise de *big data* geralmente utiliza algoritmos de aprendizagem automática, um subcampo da IA que permite que os algoritmos aprendam autonomamente a partir dos dados utilizados para o seu treino, sendo que a precisão do algoritmo aumenta com a quantidade e qualidade dos dados utilizados no treino. Esses algoritmos interpretam autonomamente o contexto e atualizam os modelos a cada decisão, aumentando gradualmente sua exatidão. Eles são usados para descobrir padrões e correlações nos dados, como a probabilidade um indivíduo ser reincidente criminal, por exemplo (Costa, 2021).

Neste contexto, é estabelecido que a IA capacita sistemas a interpretar o ambiente ao seu redor e solucionar desafios para atingir metas específicas, empregando dados previamente organizados ou obtidos pelo próprio sistema, processando-os e emitindo respostas. Esses sistemas também são capazes de adaptar sua conduta, até um certo ponto, por meio da análise autónoma. (PE, 2021a).

Os sistemas que utilizam IA podem ser divididos em duas categorias principais: aqueles que operam puramente no mundo virtual, por meio de *software*, e aqueles que são integrados nos dispositivos físicos. No caso dos sistemas virtuais, temos assistentes de voz, programas de análise de imagens, motores de busca, sistemas de reconhecimento facial e de discurso. Esses sistemas utilizam algoritmos e modelos de IA para realizar tarefas específicas, como responder a comandos de voz, identificar objetos em imagens, procurar informações na *web* ou reconhecer rostos e vozes. Já os sistemas físicos, por sua vez, integram a IA em dispositivos concretos. Exemplos incluem robôs avançados, carros autónomos, *drones* e aplicações da Internet das Coisas. Nesses casos, a IA é incorporada aos componentes do dispositivo para permitir a tomada de decisões autónomas, a interação com o ambiente e a execução de tarefas específicas. Essa integração de IA em dispositivos físicos permite que eles sejam mais autónomos, adaptáveis e capazes de interagir com o mundo real de maneira inteligente, com base em perceções e análises em tempo real dos dados do ambiente (Costa, 2021).

Outra distinção importante, é estabelecer se o sistema é simplesmente automatizado ou verdadeiramente autónomo. Em outras palavras, o sistema pode realizar tarefas baseadas em regras preestabelecidas, operando de forma automatizada e com pouca autonomia. Ou, no entanto, o sistema também tem a capacidade de controlar a maneira como executa essas

tarefas, demonstrando um certo nível de autonomia e sendo classificado como completamente autónomo. (Morgan et al., 2020, p. 9).

Morgan et al. (2020) ressalva ainda o avanço na criação de sistemas mais avançados, que possuem a capacidade de aprendizagem automática e de aprimorar continuamente a sua performance ao identificar padrões em alargados conjuntos de dados e da adoção de medidas corretivas para melhorar a capacidade de classificar padrões em situações futuras, sem exigir programação específica. Esses sistemas incluem uma classe de sistemas ainda mais sofisticados, com a capacidade de aprender em profundidade, que se apoia em redes neurais profundas, que impulsionaram avanços notáveis em sistemas de visão computacional e reconhecimento de imagens. Isso suscita questões pertinentes relacionadas com o controlo e monitorização desses sistemas, e à responsabilidade pelos resultados, com o grau de participação humana sendo um fator essencial.

Atualmente a utilização do *big data* tem tido bastante preponderância em diversas áreas da sociedade, como por exemplo para fins "publicidade comportamental, na previsão e adequação de preços, na previsão da probabilidade de cumprimento de contratos de mútuo, na avaliação de risco" e ainda, em termos de criminalidade, "o cálculo da probabilidade de reincidência de criminalidade pelos tribunais" e "a previsão de locais mais propensos à ocorrência de crimes" (Costa, 2021, p.39).

Conforme refere ainda Albuquerque (2021), na proposta de Regulamento 2021/006 (COD), que está a ser analisado e discutido pelos Estados-Membros para estabelecer regras padronizadas sobre o uso de IA, essa iniciativa procura cumprir o segundo objetivo do Livro Branco, que é desenvolver um ecossistema confiável sustentado por um quadro jurídico que promova a confiança na IA. O objetivo é lidar com desafios como a falta de transparência, a complexidade, os vieses e a imprevisibilidade de determinados sistemas de IA, com o propósito de assegurar a conformidade com os Direitos Fundamentais da UE e simplificar a execução das leis.

Os avanços dos sistemas de videovigilância combinam a recolha de imagens com a capacidade de análise e criação de alertas ou ações, com base nos resultados obtidos, o que impulsiona significativamente as operações de segurança (Security Magazine, 2021). Neste sentido, a utilização da IA desempenha um papel importante no combate à criminalidade, aumentando as capacidades de investigação através da análise de grandes conjuntos de dados e da aptidão para identificar padrões. Entretanto, a sua aplicação exige o cumprimento rigoroso dos mais altos padrões de conformidade com as diretrizes legais, garantindo, ao

mesmo tempo, uma proteção efetiva dos direitos dos cidadãos e o controle humano subjacente, especialmente nas decisões que possam afetá-los (Albuquerque, 2022).

3.3. Inteligência Artificial e a videovigilância

Como foi referido anteriormente, a IA é uma área em crescimento na sociedade, esta estando a ser aplicada em diversos setores, incluindo a videovigilância onde a mesma apresenta diversas potencialidades.

Nessa conjuntura, de acordo com Vu (2018), houve avanços significativos no desenvolvimento e aprimoramento das tecnologias de reconhecimento facial. Essas técnicas surgiram como uma resposta à limitação do cérebro humano em processar, memorizar e reconhecer a grande quantidade de rostos com os quais nos deparamos diariamente. No entanto, especialmente após os ataques terroristas ocorridos nos Estados Unidos em setembro de 2001, as instituições governamentais têm utilizado todas as ferramentas disponíveis para desenvolver métodos eficazes e precisos de controlar o fluxo de pessoas através da identificação individual. Isso tem sido feito com o propósito de garantir que nenhuma ameaça identificada seja tolerada.

Apesar do reconhecimento facial ser já uma realidade, a “recolha de dados biométricos para efeitos de identificação à distância” (CE, 2020, p. 24) pode representar riscos para os direitos fundamentais. As consequências relacionadas com os direitos fundamentais resultantes da utilização de sistemas de IA, para a identificação biométrica à distância, podem diferir consideravelmente, dependendo da finalidade, do contexto e da extensão do uso. (CE, 2020).

Segundo Hanmann e Smith (2018), o reconhecimento facial funciona da seguinte forma: geralmente, a tecnologia de reconhecimento facial cria um "modelo" da imagem facial do alvo e compara o modelo com fotografias de imagens pré-existentes de um ou mais rostos (conhecidos). As fotografias conhecidas são encontradas em diversas fontes, incluindo bancos de dados de cartas de condução, registos de identificação governamentais, fichas criminais ou contas de redes social, como por exemplo o *Facebook*, *Instagram,* ou mesmo o *LinkedIn,* entre todas as outras redes sociais que existem. Esta tecnologia utiliza uma aplicação de software para criar um modelo, analisando imagens de rostos humanos a fim de identificar ou verificar a identidade de uma pessoa. O reconhecimento facial tem o potencial de ser uma ferramenta útil no combate ao crime, na identificação meliantes capturados nas imagens de vigilância, na localização de fugitivos procurados em multidões ou na deteção de terroristas ao entrarem no país.

Refere a CE (2020) que, o reconhecimento facial pode ser utilizado para identificação ou autenticação. No processo de identificação, a imagem facial de uma pessoa é comparada com muitos outros modelos armazenados em uma base de dados para verificar se essa pessoa está presente na base de dados. Já a autenticação (ou verificação) é uma comparação "um a um" entre dois modelos biométricos, geralmente supostos pertencer à mesma pessoa. Essa comparação é efetuada com o propósito de confirmar se a pessoa presente em ambas as imagens é a mesma, e é frequentemente utilizada em portas de embarque com controlo automatizado de fronteira (*Automated Border Control*, ou *ABC*) em aeroportos para controlo de fronteiras.

A utilização da IA na videovigilância desempenha um papel significativo na previsão e prevenção de crimes. A análise de comportamento baseada em IA pode ajudar a identificar atividades suspeitas capturadas pelas câmaras de vigilância, permitindo uma resposta rápida por parte das autoridades. Na realidade a IA pode analisar movimentos suspeitos, comportamentos agressivos e outros padrões anormais que podem indicar a ocorrência de crimes iminentes. A tecnologia de reconhecimento facial é um programa de computador desenvolvido para detetar e reconhecer faces humanas específicas, a partir de imagens estáticas ou vídeos. Com o uso de bases de dados abrangentes e conexões de internet de alta velocidade, essas tecnologias têm a capacidade de reconhecer e registar características individuais para análise de imagens capturadas por computadores, *smartphones* ou sistemas de videovigilância, a utilização desta tecnologia permite a identificação rápida de indivíduos procurados ou suspeitos. Os dados processados podem ser utilizados para uma ampla variedade de finalidades (Nabeel, 2019).

A maior preocupação com o armazenamento de dados biométricos/reconhecimento facial, surge quando esses dados são comprometidos. Atualmente, os *hackers* possuem várias maneiras de manipular o sistema de forma antiética. A sua capacidade de apresentar recriações cosméticas no scanner biométrico, sobrepor o processo de extração de características ou corromper o próprio mecanismo de correspondência tem o potencial de levar esse sistema ao fracasso (Vu, 2018, p. 13). Quando comprometidos, o roubo de identidade torna-se uma grande preocupação, especialmente à medida que a biometria continua a expandir-se em áreas relacionadas à segurança e ao governo. Atualmente, existem poucas maneiras pelas quais certos dados biométricos podem ser usados maliciosamente, mas em termos de questões internacionais, em que esses dados protegem informações sensíveis destinadas a serem mantidas fora das mãos de criminosos, eles ainda representam uma ameaça que deve ser adequadamente abordada (Vu, 2018).

No entanto, é importante ressaltar que a utilização da IA na videovigilância levanta questões éticas e de privacidade e por isso, deve ser garantida a transparência, responsabilidade e proteção dos dados pessoais durante a implementação destas tecnologias, conforme destacado por Floridi et al. (2018).

3.4. Inteligência Artificial e os dados pessoais

Dizem Kissinger et al. (2021, p. 142) "nenhuma grande potência pode dar-se ao luxo de ignorar a dimensão de segurança da IA".

De acordo com o primeiro princípio relativo ao tratamento de dados pessoais preservado no RGPD, al. a) do n. º 1 do art.º 5º, os dados pessoais são "objeto de tratamento lícito, leal e transparente em relação ao titular dos dados" (UE, 2016, p. 35). A análise de *big data* é às vezes caracterizada como sinistra, uma ameaça à privacidade, ou simplesmente "assustadora". Isso ocorre porque envolve o reaproveitamento de dados de maneiras inesperadas, o uso de algoritmos complexos e a formulação de conclusões sobre indivíduos com efeitos inesperados e, às vezes, indesejáveis (Information Comissioner's Office, 2017).

O RGPD inclui disposições específicas relacionadas ao processo de definição de perfis, que é definido no seu art.º 4º, n. º 4, *definição de perfis* refere-se a qualquer processo automatizado de tratamento de dados pessoais que envolva a utilização desses dados para avaliar aspetos específicos de um cidadão, como "analisar ou prever aspetos relacionados com o seu desempenho profissional, a sua situação económica, saúde, preferências pessoais, interesses, fiabilidade, comportamento, localização ou deslocações" (UE, 2016, p. 33). Esse processo visa obter informações detalhadas sobre o indivíduo, com base em dados recolhidos e analisados automaticamente, a fim de criar um perfil ou retrato detalhado das suas características e comportamentos. Essa prática pode ser usada para diversos fins, como segmentação de mercado, personalização de serviços ou tomada de decisões automatizadas, tendo por base a utilização de IA (EU, 2016; Information Comissioner's Office, 2017).

Conforme nos diz a InternationlIT (2023) a IA "tem se mostrado uma tecnologia revolucionária em diversos campos, e a área de Tecnologia da Informação não é exceção". A IA pode ser utilizada para monitorar e analisar padrões de dados em tempo real. Algoritmos de aprendizagem de máquina podem detetar comportamentos atípicos e desvios que podem sugerir atividades suspeitas ou violações de segurança. Isso permite uma deteção mais rápida de ameaças e uma resposta proativa para proteger os dados. A IA tem sido de suma importância na luta contra o *ransomware*, um tipo de *malware* que codifica os dados de uma organização e requer um resgate para desbloquear o acesso aos arquivos. A IA

desempenha um papel essencial nesse contexto, fornecendo soluções efetivas para enfrentar esse desafio de cibe rsegurança (InternationlIT, 2023).

Segundo Frąckiewicz (2023), os sistemas baseados em IA desempenham um papel fundamental não apenas na deteção e resposta a ameaças cibernéticas, mas também na melhoria da segurança. Através da implementação de IA, é possível fortalecer diversos aspetos relacionados à segurança. Por exemplo, os sistemas baseados em IA têm a capacidade de gerar senhas mais robustas, identificar e lidar com atividades suspeitas por parte dos usuários, bem como produzir chaves de criptografia mais eficientes e seguras. Essas abordagens são essenciais para aprimorar a proteção e resiliência dos sistemas utilizados, com o fim último da proteção de dados.

PARTE II – ENQUADRAMENTO METODOLÓGICO E TRABALHO DO CAMPO

CAPÍTULO 4 - METODOLOGIA, MÉTODOS E MATERIAIS

4.1.Introdução

O presente trabalho de investigação científica tem como objetivo analisar os desafios da utilização dos sistemas de videovigilância em espaço público, utilizando as novas tecnologias que lhes estão inerentes.

Neste capítulo, é abordada a metodologia fundamental adotada nesta investigação, bem como a abordagem do problema de investigação, a análise e os métodos e técnicas empregues para a recolha, processamento e análise de dados.

O objetivo final de uma investigação científica é geralmente a procura por uma compreensão mais aprofundada dos significados de um evento ou comportamento, avaliar a situação de forma inteligente e entender de forma mais aprofundada as dinâmicas de funcionamento de uma organização específica (Quivy & Campenhoudt, 2005). Para alcançar esse objetivo, esta investigação seguiu um método sistemático que envolveu a recolha de informações concretas e comprováveis do mundo empírico. Esses dados foram usados para descrever, explicar, fazer previsões ou controlar diferentes fenómenos (Fortin, 2009). O método científico consiste numa série de etapas ou técnicas cognitivas empregues na investigação. Ele representa a sequência de ideias adotada no processo de investigação (Prodanov & Freitas, 2013).

4.2. Método de Abordagem, Estratégia de Investigação e Desenho de Pesquisa

Esta dissertação, pelo facto de que são escassos os estudos realizados em Portugal em torno da utilização dos sistemas de videovigilância, e ainda serem poucos os especialistas com conhecimento na área, é um estudo exploratório que segue uma abordagem qualitativa, tendo o seu propósito de "investigar ideias, de descobrir significados nas ações individuais e nas interações sociais a partir da perspetiva dos atores intervenientes no processo" (Coutinho, 2013, p. 28). Parte-se da premissa de que os resultados obtidos são fruto da utilização de métodos que enfatizam a análise interpretativa em vez de procedimentos estatísticos, procurando-se obter acesso a significados pessoais relacionados com experiência humana e compreender as relações e processos típicos de determinadas circunstâncias contextuais (Strauss & Corbin, 1998; Denzin & Lincoln, 2003).

Um estudo exploratório, tem como objetivo principal a familiarização do investigador com o assunto investigado. Este é realizado quando o tema é pouco conhecido ou pouco estudado, e procura gerar hipóteses e ideias para investigações mais aprofundadas no futuro. Geralmente, um estudo exploratório envolve a recolha de dados de diversas fontes, como entrevistas com especialistas, levantamento bibliográfico e análise de documentos. Os resultados são descritos de forma qualitativa, sem a pretensão de generalização ou comprovação de hipóteses. O estudo exploratório é útil para orientar futuras pesquisas, pois ajuda a definir as questões mais relevantes a serem investigadas e os métodos mais adequados para alcançar os objetivos da investigação. Além disso, permite a identificação de lacunas no conhecimento sobre o tema, que podem ser exploradas em investigações futuras (Creswell, 2009).

A abordagem construtivista tem como pressuposto teórico que o conhecimento é construído pelo indivíduo a partir de sua experiência e das interações sociais que estabelece. Nessa abordagem, o investigador assume uma postura participativa, procurando entender como os indivíduos constroem os seus conhecimentos e como estes conhecimentos são aplicados na prática. (Vygotsky & Cole, 2018)

Ainda referem Vygotsky e Cole (2018), que o construtivismo postula que o conhecimento não é uma mera reprodução da realidade, mas sim uma construção social que é influenciada por fatores individuais e coletivos. Dessa forma, o investigador que utiliza essa abordagem deve levar em consideração as perspetivas e experiências dos participantes, procurando compreender como eles constroem o próprio conhecimento e como este conhecimento é aplicado na prática.

Deste modo, optou-se pela abordagem construtivista para a realização deste estudo, uma vez que esta abordagem permitirá compreender a videovigilância e os desafios à sua aplicabilidade. Além disso, a abordagem construtivista permitirá entender como as interações sociais e as experiências individuais dos participantes influenciam na construção de seus conhecimentos.

Ao decidir o problema de pesquisa, é importante escolher uma estratégia de investigação e o desenho de pesquisa adequados (Santos, et al., 2019). Neste estudo em particular, optou-se pela estratégia qualitativa e pelo método de estudo de caso respetivamente.

Optando por uma abordagem qualitativa, permite ao investigador uma "compreensão absoluta e ampla do fenómeno em estudo. Ele observa, descreve, interpreta e aprecia o meio e o fenómeno tal como se apresentam, sem procurar controlá-los" (Fortin, 1999, p.22). Nessa

abordagem, é pressuposto que o conhecimento é construído a partir da experiência, e cabe ao investigador, por meio de técnicas como entrevistas, obter e interpretar as experiências relatadas pelos participantes da pesquisa (Renda, Ribeiro, & Baleiro, 2017). E ainda relativamente ao encontro entre a abordagem qualitativa e ao estudo de caso, que "procura recolher informação detalhada sobre uma única unidade de estudo, podendo essa unidade ser o indivíduo, a comunidade ou até mesmo a nação" (Santos, et al, 2019, p.36).

Rosado (2015) identificou três métodos de pesquisa: o método dedutivo, o método indutivo e o método hipotético-dedutivo. Nesta investigação, optou-se pelo uso do método dedutivo, que se caracteriza por partir de uma premissa geral para a formulação de hipóteses específicas que serão testadas por meio de evidências empíricas. O método dedutivo, "a partir de princípios, leis ou teorias consideradas verdadeiras e indiscutíveis, prediz a ocorrência de casos particulares com base na lógica" (Prodanov e Freitas 2013, p.27). Esse raciocínio é composto por três etapas: a formulação de hipóteses ou premissas, a inferência que transforma as hipóteses em uma tese e a conclusão final (Santos, et al., 2019).

Na presente investigação partiu-se do geral para o específico, iniciando com o ordenamento jurídico internacional, relevante para a temática, no âmbito dos direitos humanos, de seguida foram abordadas as leis e regulamentos emanados pela UE, e por fim, a legislação nacional referente à temática abordada, tanto da videovigilância policial, como também da proteção de dados. De seguida, foi abordado mais especificamente a videovigilância, a sua evolução, o conceito de videovigilância policial, a IA nos sistemas de videovigilância e ainda a aplicabilidade que estes sistemas têm. Modelo de Análise

Diz-nos Fortin (2009, p.23) que o "rigor e a sistematização que devem estar presentes em qualquer investigação", neste subcapítulo será abordada a metodologia que o investigador utilizou na realização da presente investigação, pelo que a escolha de determinada metodologia deve ser realizada tendo por base o problema da investigação e não as capacidades do investigador (Neves & Guerra, 2015). Assim, irá ser exposto o modelo de análise onde está explanado o Objetivo Geral da investigação, assim como a Pergunta de Partida e as Perguntas Derivadas, o desenho da pesquisa e a técnica de recolha e tratamento de informação.

Para que uma investigação tenha carácter científico, a mesma deve atender a determinadas condições, como a definição clara de um objeto de estudo, uma perspetiva original que oriente a investigação desse objeto, a relevância científica do estudo e a obtenção de resultados que permitam confirmar ou refutar as questões de pesquisa, contribuindo assim para a produção de conhecimento (Eco, 2007). A metodologia pode-se

designar como o "corpo orientador da pesquisa que (…) torna possível a seleção e articulação de técnicas, no intuito de se poder desenvolver o processo de verificação empírica" (Pardal & Correia 1995, p. 10).

De forma que a investigação tenha um fio condutor e que tenha um prepósito, deve-lhe ser designado um Objetivo Geral (OG), assim, e tendo em conta o objeto de estudo: "Aplicações tecnológicas nos sistemas de videovigilância policial", para esta investigação foi definido o seguinte:

OG: "Avaliar os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos".

Este deve estar intimamente ligado com a Pergunta de Partida (PP), como nos diz Sarmento (2013), o processo de investigação deve começar pela fase exploratória, definindo a PP e as perguntas derivadas (PD). A PP é a questão que deve estar alinhada com o título e a temática do estudo, e deve ser clara, unívoca, concisa, direta, precisa, relevante, inovadora, exequível e, por fim, compreensiva ou explicativa. (Rosado, 2017). Portanto pretende-se com a investigação responder à mesma

PP: "Quais os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos?"

Para concretizar o OG e responder à PP, surgem então as PD, que se relacionam intimamente com os OE, assim as mesma devem ser, como indica "enunciados interrogativos precisos, escritos no presente" (Fortin, 2009, p. 101):

PD1 - Qual o ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos?

PD2 - Que aplicações tecnológicas podem ser admissíveis nos sistemas de videovigilância policial em espaços públicos?

PD3 – Que aplicabilidade tem a Inteligência Artificial nos sistemas de videovigilância policial em espaços públicos?

De forma a ser facilmente consultado, encontra-se no apêndice A o Modelo de Análise, onde está explanado a inter-relação entre os conceitos abordados nesta pesquisa, suas dimensões e as técnicas de recolha e análise de dados utilizadas para abordar as perguntas de pesquisa e os objetivos específicos relacionados a esses conceitos.

4.3. Técnica de Recolha e Tratamento de dados

A recolha de dados, no enquadramento conceptual, teve por base fontes de origem primária e secundária. Nas fontes primárias foram utilizados documentos institucionais de

acesso público, legislação nacional e internacional, livros, artigos e revistas científicas. Como fontes secundárias foram utilizados artigos e revistas científicas.

Para ir de encontro a esses dados, foram utilizadas diversas bases de dados, incluindo EBSCO, B-On, RCAAP e *Google* Académico. Para focar a pesquisa na temática em questão, foram selecionadas palavras-chave como: "Sistemas Videovigilância"; "Videovigilância policial"; "Evolução da videovigilância"; "Inteligência Artificial"; "GNR/Videovigilância"; "Policiamento preditivo"; "Reconhecimento facial" e "Proteção de dados".

Na fase empírica, que se baseia numa abordagem qualitativa, os dados foram recolhidos por meio de entrevistas. Tendo em conta as questões e objetivos da investigação e com base nos dados obtidos durante a fase conceptual, a entrevista permite que o investigador expresse suas perceções ao entrevistado, fazendo perguntas abertas para obter respostas autênticas e profundas (Quivy & Campenhoudt, 2005).

Para a presente investigação foram realizados inquéritos por entrevistas semiestruturadas, a diversas entidades com conhecimento e experiência na área. Estas entrevista foram conduzidas de forma a manter uma conversa com os entrevistados, colocando questões-guias, abertas, para que o mesmo tivesse espaço para desenvolver as suas respostas. O trabalho do investigador nesse momento, será manter e reencaminhar a entrevista para aquilo que são os objetivos da investigação quando o entrevistado se afaste destes, existindo também a possibilidade de novas perguntas, que derivam das respostas do entrevistado (Quivy & Campenhoudt, 2005). Estas entrevistas tiveram também um caracter confirmatório, que, ao contrário das entrevistas exploratórias, estas servem para validar informações já obtidas na revisão da literatura (Sarmento, 2013)

Ainda foi enviado o consentimento informado aos entrevistados, este é um processo pelo qual o investigador explica aos participantes da investigação os objetivos, procedimentos, riscos e benefícios da pesquisa, de forma clara e compreensível, e solicita a permissão para que o participante possa participar voluntariamente da pesquisa. O objetivo do consentimento informado é garantir que os participantes da pesquisa estejam cientes do que a pesquisa envolve e que estejam dispostos a participar livremente, sem qualquer forma de coerção ou pressão externa. Isso inclui esclarecer qualquer risco potencial para a privacidade e confidencialidade do participante, e permitir que o participante faça perguntas e esclareça dúvidas antes de decidir se deseja ou não participar da investigação.

O Guião de Entrevista é constituído por três grandes blocos de temas de perguntas, as quais abordam os Objetivos Específicos: OE; OE2 e OE3.

4.4. Amostra

De modo a se obter os melhores dados para a investigação, nesta investigação foi utilizada uma amostragem intencional, que procura entrevistados com experiência na área. É pertinente que os entrevistados tenham conhecimentos e experiência sobre o tema a ser abordado. A amostra é "uma porção ou parcela, convenientemente selecionada do universo (população); é um subconjunto do universo" (Lakatos e Marconi, 2003, p. 163),

Creswell (2018) afirma que a amostragem intencional pode ser uma escolha apropriada em pesquisas qualitativas quando o objetivo é entender as experiências, perspectivas e opiniões de um grupo específico de pessoas, como profissionais com experiência na área. Nesse tipo de amostragem, o investigador seleciona os participantes com base em critérios específicos que são relevantes para a pesquisa, como a experiência na área, a posição ocupada na organização, a formação acadêmica, entre outros. O objetivo é obter participantes que tenham conhecimento e experiência relevantes para responder às perguntas da entrevista de forma mais precisa e completa.

Assim, e tendo por base o que foi supramencionado, durante a investigação foi lançado um inquérito por entrevista para um grupo de pessoas. Esses indivíduos, especialistas e com experiência na área da videovigilância, foram selecionados com o intuito de apurar o contexto e eventuais potencialidades e vulnerabilidades. A amostra utilizada nesta entrevista é a que se apresenta na Tabela 2:

Tabela 2 - Composição da amostra

Identificação dos entrevistados				**Local**	**Data**
Código	**Posto/Grau Académico**	**Função**	**Instituição**		
E1	Dr.	Responsável de vendas	Empresa na área da segurança	Vídeo conferência	21ABR23
E2	Tenente-Coronel	SOTRP de CTer	GNR	Vídeo conferência	26ABR23
E3	Tenente-Coronel	SIIC	GNR	Comando Geral da GNR	07MAI23

E4	Major	Repartição de Operações do Comando Operacional	GNR	Comando Geral da GNR	08MAI23

Fonte – Elaboração própria

Um dos entrevistados é o responsável de vendas de uma empresa que trabalha na área da segurança, relacionada com a segurança física, controlos de acessos e videovigilância, e tudo o que seja inerente a essas tecnologias, nomeadamente análise de vídeo e outras funcionalidades como reconhecimento facial ou leitura de matrículas. Os outros três entrevistados são Oficiais Superiores que têm experiência na implementação de sistemas de videovigilância policial em espaço público, no território português.

Foi também observado o critério da saturação através da recolha sucessiva de informação até à saturação teórica, ou seja, até ao momento em que a aplicação das entrevistas não surgem novas informações ou contributos.

CAPÍTULO 5 – APRESENTAÇÃO, ANÁLISE E DISCUSSÃO DE RESULTADOS

5.1. Introdução

Neste capítulo, são apresentados, analisados e discutidos os dados obtidos por meio dos inquéritos por entrevista. Inicialmente, são apresentados os dados recolhidos e realizada uma análise qualitativa e quantitativa das entrevistas, identificando os principais temas abordados. Em seguida, os dados são interpretados e discutidos, comparando-os com a revisão de literatura realizada nos Capítulos Um, Dois e Três.

5.2. Apresentação e discussão de resultados

Com o intuito de oferecer uma análise mais aprofundada e uma apresentação mais precisa das categorias e subcategorias resultantes da análise das entrevistas, esta investigação optou por apresentar os conteúdos de todas as entrevistas em forma de tabela, para de seguida serem discutidos os resultados e comparados com a revisão da literatura.

A primeira etapa do processo consistiu na identificação das categorias e subcategorias, apresentadas na tabela abaixo. Isso possibilitará um acesso mais facilitado ao conteúdo desejado. Posteriormente, foi elaborada uma matriz de análise de conteúdo, estabelecendo a relação entre cada subcategoria e os participantes das entrevistas, as Unidades de Enumeração (UE) e os resultados obtidos para cada questão da entrevista. Dessa forma, procurou-se analisar e organizar os dados de maneira quantitativa e qualitativa, proporcionando uma análise mais clara e compreensível.

Tabela 3 - Análise quantitativa e qualitativa das entrevistas

Categoria	Subcategoria	Entrevistados				EU	Resultado
		E1	E2	E3	E4		
Pergunta 1 - Qual a legislação em vigor que regula a utilização de sistemas de videovigilância policial em espaços públicos pelas Forças de Segurança?							
Ordenamento Jurídico	Legislação Nacional (Videovigilância)	X	X	X	X	4	4/4 (100%)
	Legislação Nacional (Dados pessoais)	X	X	X	X	4	4/4 (100%)
Pergunta 2 - Quais as principais exigências legais para a implementação dos sistemas de videovigilância policial em espaços públicos?							
Ordenamento Jurídico	Autorização CNPD	X	X	X		3	3/4 (75%)
	Privacidade	X	X	X	X	4	4/4 (100%)
	Sinalização			X	X	2	2/2 (50%)

Pergunta 3 - Quais as lacunas que identifica no ordenamento jurídico em vigor que regula a utilização de sistemas de videovigilância policial?							
Lacunas	Especificidade	X	X	X		3	3/4 (75%)
	Dados Biométricos/ Reconhecimento facial	X	X		X	3	3/4 (75%)
	Dados Pessoais			X		1	1/4 (25%)
Pergunta 4 - Quais os pontos fortes e fracos do ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos?							
Ordenamento Jurídico Pontos Fortes	Proteção de Dados	X	X		X	3	3/4 (75%)
	Autorização Prévia CNPD	X	X	X	X	4	4/4 (100%)
Ordenamento Jurídico Pontos Fracos	Proteção de Dados			X	X	2	2/2 (50%)
	Falta de Especificidade	X	X	X	X	4	4/4 (100%)
Pergunta 5 - Que tipo de aplicações tecnológicas podem e devem ser aplicadas nos sistemas de videovigilância policial em espaços públicos?							
Aplicações	Sistemas Integrados com a Videovigilância	X		X		2	2/2 (50%)
	Analítica de vídeo	X	X	X	X	4	4/4 (100%)
	Reconhecimento Facial	X		X		2	2/2 (50%)
Pergunta 6 - Com a evolução da tecnologia e a implementação da Inteligência Artificial em diversos setores, de que forma poderá esta ser utilizada nos sistemas de videovigilância policial, de acordo com o ordenamento jurídico em vigor?							
Inteligência Artificial	Sistema de Alarmística	X	X	X	X	4	4/4 (100%)
	Analítica de vídeo	X	X	X	X	4	4/4 (100%)
Pergunta 7 - No domínio do tratamento e análise de dados, quais as especificações técnicas dos equipamentos de videovigilância que poderão afetar a privacidade das pessoas, em particular os seus Direitos, Liberdades e Garantias, e de que forma poderá este problema ser impedido?							
Especificidades que afetam os DLG	Dados Biométricos/ Reconhecimento Facial	X	X	X		3	3/4 (75%)
Solução	Seleção dos Equipamentos		X		X	2	2/2 (50%)
	Proteção de Dados	X	X	X	X	4	4/4 (100%)
Pergunta 8 - Quais as Vantagens/oportunidades podem ser apontadas à utilização dos sistemas de videovigilância com IA?							
Vantagens/ Oportunidades	Prevenção	X	X	X	X	4	4/4 (100%)
	Eficácia da Atuação das FSS	X	X	X	X	4	4/4 (100%)
	Redução no Tempo de Atuação das FSS	X	X	X		3	3/4 (75%)
	Redução de RH	X		X		2	2/2 (50%)
Pergunta 9 - Quais as desvantagens/ameaças podem ser apontadas à utilização dos sistemas de videovigilância com IA?							
Desvantagens/ Ameaças	Utilização Indevida	X	X		X	3	3/4 (75%)
	Investimento		X	X		2	2/2 (50%)
	Discriminação	X		X	X	3	3/4 (75%)

Fonte: Elaboração própria

Foi verificado na tabela acima, que quinze subcategorias, das vinte e oito, originadas a partir das respostas dos entrevistados, não atinge o total de respostas por toda a amostra. As subcategorias restantes receberam uma percentagem total de respostas por parte dos entrevistados, o que indica que os objetivos de cada questão foram alcançados.

A etapa seguinte consiste na discussão de resultados, esta foca-se nas categorias e subcategorias criadas para a análise das entrevistas, como tal segue a seguinte análise:

Na primeira subcategoria, **Legislação Nacional (Videovigilância)**, da categoria **Ordenamento Jurídico**, três dos entrevistados referem a legislação pela qual a videovigilância é regulada, estes referem a Lei n.º 95/2021, de 29 de dezembro, "a Lei n.º 95/2021, de 29 de dezembro, que revogou a lei 1/2005" (E2), que regula a utilização e o acesso pelas forças e serviços de segurança aos sistemas de videovigilância. Para regular os requisitos técnicos mínimos das câmaras fixas e portáteis de videovigilância apenas um entrevistado refere as Portarias n.º 372/2012 e n.º 373/2012, ambas de 16 de novembro, "deve existir avisos à entrada dos locais onde esse sistema está a ser utilizado (…) isto é um requisito da lei 59/2019, para isso importa também referir as portarias n.º 372/2012 e n.º 373/2012, ambas de 16 de novembro" (E4). De acordo com a revisão da literatura, constata-se que a legislação vigente que estabelece diretrizes para a aplicação da videovigilância por parte das FFSS é precisamente a mesma mencionada pelos entrevistados.

Na subcategoria **Legislação Nacional (dados pessoais),** todos os entrevistados referem a Lei n.º 59/2019, de 8 de agosto, "nomeadamente a Lei n.º 59/2019, de 8 de agosto, para a proteção de dados" (E1), referente aos dados pessoais para prevenção, deteção, investigação ou repressão de infrações penais. No entanto apenas o E4 refere a Lei n.º 58/2019, de 8 de agosto, "esta assegura a execução, na ordem jurídica nacional, do RGPD, que é o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho" (E4). No âmbito dos dados pessoais, a revisão da literatura corrobora as afirmações dos entrevistados, atestando que a legislação nacional que regula também a proteção de dados pessoais e a privacidade é a mesma mencionada por eles.

Quanto à subcategoria, **Autorização CNPD**, verifica-se que três dos entrevistados referem a CNPD como sendo a entidade que autoriza a implementação dos sistemas, "antes da instalação do sistema de videovigilância, é necessário obter uma autorização prévia da CNPD" (E3), mas é importante referir que "o parecer da CNPD não é vinculativo, no entanto maior parte das vezes é assim seguido as suas indicações a 100%" (E1), o E3 ainda acrescenta que a CNPD "irá avaliar se o sistema respeita os direitos fundamentais e as liberdades públicas, nomeadamente a privacidade e a proteção de dados pessoais" para emitir

o seu parecer. Para a instalação de um sistema de videovigilância, em consonância com a revisão da literatura, não sendo vinculativo, é, no entanto, necessário o parecer da CNPD, para tal preciso fundamentar a necessidade desse sistema, identificar o locar e área abrangida pela captação, assim com os pontos de instalação das câmaras, entre outras informações essenciais para se obter um parecer positivo da CNPD.

Já na subcategoria **Sinalização**, apenas dois entrevistados referem as portarias que regulam a sinalização das câmaras de videovigilância "poderá ainda realçar-se os requisitos exigidos nas Portarias n.º 372/2012 e n.º 373/2012, ambas de 16 de novembro" e também "a instalação e o funcionamento dos sistemas de videovigilância devem ser sinalizados de forma clara e visível, para que as pessoas que se encontram no local tenham conhecimento da sua existência" (E3), também estas portarias mencionadas no primeiro capítulo.

Dentro da subcategoria **Privacidade**, consta-se que, é consensual em todos os entrevistados que a legislação deve proteger a privacidade do cidadão, "é necessário fazer uma avaliação de impacto à lei de proteção de dados, verificar aonde se enquadra esta instalação" (E2), "invoca-se a necessidade de proteção de dados pessoais, em especial os dados biométricos" (E4).

Relativamente à subcategoria **Especificidade**, da categoria Lacunas, três entrevistados referem que a lei deveria ser mais específica, tanto quanto às limitações, bem como às possibilidades "na lei 95, onde nos fala da parte da análise inteligente de vídeo, no entanto não denota qual é a análise de vídeo que se deve utilizar e em que ambiente se utiliza a decisão analítica" (E1), "é necessário uma regulamentação mais detalhada que preveja, por exemplo, as condições específicas de utilização dos sistemas de videovigilância em locais de elevado risco ou em eventos de grande dimensão" (E3). Nesta subcategoria os entrevistados acrescentaram informações que não foram verificadas na investigação, acrescentando assim conhecimento.

Nos **Dados biométricos/Reconhecimento facial**, foi verificado que esta tecnologia existe e pode ser aplicada nos sistemas de videovigilância, no entanto, devido à legislação portuguesa sobre a matéria, é proibida a utilização deste. Ainda que, três dos entrevistados refiram a importância da utilização do reconhecimento facial para a atividade policial, "outro ponto que tem uma falha relativamente ao reconhecimento facial (…) que possibilite dissuadir o crime e evitar a perpetuação de novos crimes" (E1), e ainda acrescenta o E3 que o reconhecimento facial "pode ser usado para identificar pessoas procuradas pela justiça ou suspeitas de cometer crimes, permitindo uma intervenção policial mais rápida e eficaz".

Em relação aos **Dados Pessoais**, apenas o E3 refere ainda haver lacunas na Lei, referindo que "(…) há uma necessidade de reforçar essas proteções (da privacidade e da proteção de dados) para garantir que os sistemas de videovigilância não sejam utilizados de forma abusiva ou desproporcional", corroborando a importância da proteção dos dados pessoais anteriormente referido.

Relativamente ao pontos fortes do ordenamento jurídico, na subcategoria **Proteção de Dados**, todos os elementos referiram a importância do parecer da CNPD, para que sejam respeitados os direitos dos cidadão, pois "a clarificação dos aspetos essenciais de como um pedido de autorização deverá ser instruído, de forma a orientar o processo de autorização" (E4), e ainda três entrevistados referem como ponto forte a forma como a proteção de dados está regulamentada, sendo que "é vedada a utilização de câmaras de vídeo quando a captação de imagens e de sons abranja o interior de casa ou edifício habitado ou sua dependência (…) as imagens e os sons acidentalmente obtidos, devem ser destruídos de imediato pelo responsável pelo sistema" (E4), ainda é referida por dois entrevistados que a conservação dados deve ser feita pelo período de 30 dias. Conforme explorado no primeiro capítulo e ainda reforçado no subcapítulo 3.4 da presente investigação.

Relativamente à **Autorização Prévia da CNPD**, conforme referido na investigação, o parecer da CNPD é necessário para que o sistema de videovigilância a ser instalado, esteja conforme o legalmente exposto relativamente à proteção da privacidade e dos dados pessoais, sendo mencionado por todos os entrevistados a importância de tal parecer, "a autorização prévia da Comissão Nacional de Proteção de Dados, garantindo assim a proteção dos direitos fundamentais, nomeadamente a privacidade e a proteção de dados pessoais" (E3), "se quiser implementar um sistema de segurança, tenho que fazer todos os passos que a CNPD requer, neste caso para verificar o impacto na proporcionalidade" (E1).

No entanto relativamente à subcategoria dos pontos fracos na **Proteção de Dados**, o "total respeito pelos requisitos derivados do RGPD, não contribui na sua totalidade para uma efetiva prevenção criminal" (E4), refere ainda E3 que "há a necessidade de reforçar essas proteções para garantir que os sistemas de videovigilância não sejam utilizados de forma abusiva ou desproporcional", ainda é referida a importância que teria o tratamento dos dados biométricos, se este pudessem ser captados, dessa forma impulsionaria a prevenção criminal, ajudando na procura de suspeitos previamente identificados, corroborando a investigação feita, "a não possibilidade de captação e tratamento de dados biométricos, na medida em que retira da equação dados que permitiram estabelecer padrões associados a determinados fenómenos criminais" (E4). Ainda foi identificado pelos entrevistados, que a falta de

especificidade é um ponto fraco, reforçando também o que disseram quanto às lacunas na Lei, "a falta de regulamentação detalhada, a Lei n.º 53/2008 não prevê condições específicas de utilização dos sistemas de videovigilância em locais de elevado risco ou em eventos de grande dimensão as condições específicas de utilização dos sistemas de videovigilância" (E3).

Referente ao subcategoria **Sistemas Integrados com a Videovigilância,** da categoria Aplicações, "todos os sistemas podem ser integrados e podem ser de uma certa forma ajudados com outros sistemas" (E1), conforme foi visto os sistemas de videovigilância integrados com outras aplicações tecnológicas traz ainda mais benefícios para o utilizador, "ter outros elementos que possam conjugar com os sistemas de SVV não só na parte de dissuasão mas também na parte de apoio ao utilizador" (E1), ainda acrescenta a utilização de um sistema que "dá o *tracking* para ela (utilizador) seguir, e ir nas direções onde existem camaras , nesse momento que ela faz a localização, é enviada para o gabinete de controlo", desta forma quem controla as câmaras sabe que tal pessoa vai seguir determinado itinerário, e a pessoa esta salvaguardada de que se algo acontecer, esta a ser visto pela policia local. Neste âmbito ainda é referida a "tecnologia de reconhecimento de matrículas de veículos que pode ser usada para detetar veículos furtados ou usados em crimes" (E3), sendo apenas estes dois entrevistados a referir sistemas que podem ser integrados com a videovigilância.

No entanto, relativamente à **Analítica de Vídeo**, conforme foi descrita no subcapítulo 2.3 da investigação, também os entrevistados referem a importância e a potencialidade desta tecnologia ao ser utilizada em consonância com a videovigilância, "a análise do padrão da imagem, temos uma imagem onde habitualmente há movimento de pessoal, com determinada velocidade, se houver um movimento brusco o sistema dispara um alerta" (E2), "permitam analisar comportamentos e antecipar, mediante alarmística, a ocorrência de crimes" (E4).

Quanto ao **Reconhecimento Facial,** na mesma categoria, dois entrevistados referem que a utilização do reconhecimento facial seria benéfica para uma intervenção mais rápida e eficaz da polícia, no entanto esta "deve ser usada com cautela para evitar possíveis erros de identificação" (E3).

Na seguinte categoria, Inteligência Artificial, a subcategoria **Sistema de Alarmística,** todos os entrevistados partilham da mesma opinião, e conforme com o que foi revisto na investigação, a utilização algum sistema de alarmística com a videovigilância, acaba por potência esta, sendo que desta forma não é necessário empenhar o efetivo a controlar as câmaras, "(os militares) no dia-a-dia deles as tarefas são outras , e assim eles

recebem o *input* desses sistemas se ele tiver o sistema de alarmística, porque se estivermos à espera de resultados do sistemas pela capacidade de detetar coisas a olhar para as imagens, é humanamente impossível" (E2).

Quanto à subcategoria, **Análise de vídeo**, esta também foi claramente explicada a sua aplicabilidade por todos entrevistados, e assim corroborando o subcapítulo 2.3 da presente investigação, assim a "a IA pode ser usada para analisar automaticamente as imagens de videovigilância em tempo real e identificar comportamentos suspeitos, tais como movimentos rápidos, lutas, ou tentativas de esconder objetos" (E3).

Relativamente à subcategoria **Dados Biométricos/ Reconhecimento Facial,** da categoria Especificidades que afetam os DLG, é salientado por três entrevistados que as recolha de dados biométricos afetam a privacidade e vai contra a proteção de dados pessoais, conforme visto no subcapítulo 1.4. "os dados biométricos estão inibidos pela CNPD, pela diretiva comunitária e pela legislação nacional de serem tratados de uma forma automática" (E1).

Quanto à categoria Soluções, na subcategoria **Seleção de Equipamentos**, dois entrevistados referem que a solução está na especificidade dos equipamentos, "tem que haver rigor a diversos níveis, começando pelo nível dos garantes conferidos pelo equipamento selecionado e utilizado" (E2). sendo que estas solução não foi identificada na revisão da literatura.

E ainda, na subcategoria **Proteção de Dados**, é consensual que a solução esta na forma como os dados pessoais são protegidos, acrescentando o E3 que "é importante que os indivíduos sejam informados sobre a presença de equipamentos de videovigilância e sobre o uso que está a ser feito dos dados capturados" sendo que a utilização da videovigilância policial deve ser transparente para com o cidadão. Esta proteção é também deve ser no sentido da preservação dos dados "tanto pune quem guarda dados para além dos 30 dias, como quem não os guarda durante os 30 dias a que é obrigado".

Foram ainda apontadas diversas Vantagens/Oportunidades, que foram divididas nas subcategorias **Prevenção, Eficácia da Atuação das FFSS, Redução no Tempo de Atuação das FSS e Redução de RH**, foi referido a "*Conventional Neural Network*, que, essencialmente, refere-se à criação de objetos como por exemplo, pessoas, carros, bicicletas, mochilas, armas, etc. para depois serem utilizados aquando da analítica de vídeo" (E1); "a IA pode ser usada para ajudar a prevenir crimes e proteger os cidadãos" (E3), o E4 refere que "melhora a capacidade policial, maximizando o policiamento preditivo e as antecipação de comportamentos que levam à pratica de crimes", ainda o E1 acrescenta "Portanto a IA na

parte da videovigilância, é intenção reduzir o tempo de atuação das FFSS e dar maior flexibilidade em termos de inputs e elementos dissuasores". No âmbito da utilização da IA, corrobora a informação prestada pelos entrevistados, com a investigação deita anteriormente explicada no subcapítulo 2.3, e ainda no capítulo 3.

Referente à subcategoria **Utilização Indevida**, são três os entrevistados que apontam o facto da videovigilância com IA ser utilizada de forma indevida, e por esse motivo, como visto na revisão da literatura, é dada importância à proteção dos dados pessoais e ao direito à vida privada dos cidadãos, "um exemplo típico que vemos é na china, onde tem sistemas de videovigilância com IA e que eles até diferenciam as etnias das pessoas (…) o grande risco dos sistemas de IA e a sua evolução, é a liberdade" (E1);

Ainda, quanto à subcategoria **Investimento**, dois entrevistados referem ser uma desvantagem, durante a investigação não foi abordado este aspeto da videovigilância, o E2 refere que deve ser investido nos recursos humanos, de forma a dar resposta aos alertas emitidos por estes sistemas de videovigilância, para que os mesmos não percam credibilidade, "a implementação de sistemas de videovigilância com IA pode ser muito cara" (E3).

Por último na subcategoria **Discriminação,** nesta também se aplica o que disse o E3 "um exemplo típico que vemos é na china, onde tem sistemas de videovigilância com IA e que eles até diferenciam as etnias das pessoas", acrescenta "a IA pode ser afetada por preconceitos e discriminações, levando a decisões injustas e discriminatórias, especialmente em relação a grupos vulneráveis (E3). Este tipo de tecnologias, se não forem implementadas tendo em conta o fator da discriminação, quando são colocados os dados que a IA vai utilizar para aprendizagem, poderá cair no erro de ser criado um algoritmo discriminatório.

5.3. Resposta às perguntas derivadas

5.3.1. Resposta à pergunta derivada 1

Em relação à **PD1 "Qual o ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos?"**, no âmbito da legislação nacional aplicada, é importante primeiramente fazer referência aos regulamentos UE que foram transpostos para o ordenamento jurídico nacional, onde são salientados o Regulamento Geral de Proteção de Dados (Regulamento UE n.º 2016/679) e a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, estabelecendo diretrizes específicas para a proteção de dados pessoais no contexto da aplicação da Lei.

No âmbito do direito nacional, a CRP é a base jurídica fundamental que estabelece os DLG dos cidadãos. No contexto da videovigilância policial em espaços públicos, diversas leis são aplicáveis. A Lei n.º 58/2019, de 8 de agosto, que determina limitações ao uso e tratamento de dados pessoais, assegurando que a videovigilância policial seja realizada de forma proporcional e em conformidade com a legislação de proteção de dados. A Lei n.º 59/2019, de 8 de agosto, que aborda o tratamento de dados pessoais para prevenção, deteção, investigação ou repressão de infrações penais, estabelecendo diretrizes específicas nesse contexto.

Recentemente, a Lei n.º 95/2021, de 29 de dezembro, que revogou a Lei 1/2005, de 10 de janeiro, regula a utilização e o acesso a sistemas de videovigilância pelas FFSS e ANEPC, atualizando o enquadramento legal para o uso desses sistemas. Esta nova lei procura harmonizar os princípios de segurança e privacidade, estabelecendo requisitos e salvaguardas para a videovigilância policial em espaços públicos. Adicionalmente, as Portarias n.º 372/2012 e n.º 373/2012, ambas de 16 de dezembro, também são relevantes, definindo requisitos técnicos e operacionais para a instalação e utilização dos sistemas de videovigilância policial.

5.3.2. Resposta à pergunta derivada 2

A **PD2 "Que aplicações tecnológicas podem ser admissíveis nos sistemas de videovigilância policial em espaços públicos?"**, aborda o uso de tecnologia em sistemas de videovigilância policial e envolve diversas possibilidades. Quando falamos de sistemas de videovigilância pública, todos os sistemas podem ser integrados e podem ser de uma certa forma ajudados com outros sistemas. Ao longo desta dissertação verificou-se que diversas aplicações e ferramentas podem ser utilizadas em conjunto com os sistemas de videovigilância policial em espaço público, que serão a seguir apresentadas.

Outra ferramenta, é a possibilidade de através da videovigilância e dos alertas emitidos, ser possível controlar as luzes dos semáforos, de forma que, por exemplo, se um individuo conduzir de forma descontrolada ou em contramão, são colocados em vermelho os semáforos dos que conduzem em sentido contrário, ou que seriam intercedidos num cruzamento, o que faria evitar uma colisão.

É importante ressalvar que os sistemas de videovigilância podem e devem integrar com outras tecnologias que se interligam entre si. Por exemplo, podem ser utilizadas aplicações pelos cidadãos, as quais mostram itinerários seguros, onde possam estar a ser vigiados por camaras de videovigilância policial, assim se alguma emergência acontecer, a

força de segurança territorialmente competente, que controla esse sistema, estará alerta e pronta a intervir caso seja necessário. E ainda pode ser adicionado um botão de pânico, caso algo aconteça, para poderem ser localizados de forma célere.

Além das aplicações mencionadas anteriormente, outra tecnologia relevante nos sistemas de videovigilância policial em espaços públicos que poderá ser utilizada, é o reconhecimento de matrículas de veículos. Essa tecnologia permite a deteção automática e o reconhecimento das placas de matrículas de veículos, por meio de câmaras de vigilância. Esta tecnologia pode ser usada para identificar e fazer o seguimento de veículos furtados, ajudando as forças de segurança a recuperá-los mais rapidamente. Além disso, essa tecnologia é útil para identificar veículos usados em crimes, permitindo uma intervenção policial mais ágil e eficaz. Quando um veículo suspeito é detetado pelas câmaras de videovigilância e sua matrícula é reconhecida, as autoridades podem tomar medidas imediatas para investigar e impedir a continuação da atividade criminosa.

Tambem importa ressalvar as tecnologias utilizadas na proteção das florestas, neste âmbito as tecnologias de deteção mais utilizadas são: as câmaras de luz; câmaras a preto e branco, que utilizam diferenças de contraste para deteção de fumo, enquanto câmaras coloridas comparam imagens consecutivas para identificar variações de cor; câmaras com sensores térmicos; a espectroscopia ótica com espetrômetro permite a deteção automática de elementos de fumo na atmosfera, sem intervenção humana.

5.3.3. Resposta à pergunta derivada 3

Relativamente à **PD3 "Que aplicabilidade tem a Inteligência Artificial nos sistemas de videovigilância policial em espaços públicos?"** a IA pode ser aplicada nos sistemas de videovigilância policiais em espaço público, através da analítica de vídeo, pois podem ser utilizados algoritmos para detetar comportamentos suspeitos, identificar objetos deixados nalgum sítio ou reconhecer padrões de atividade incomuns. Essas ferramentas auxiliam a identificação rápida de situações potencialmente perigosas, permitindo uma resposta adequada por parte da polícia, através de um alerta que é emitido na sala onde é feito o controlo destes sistemas. Isto implica também a capacidade de monitorização em tempo real, com o uso de tecnologias de transmissão de vídeo em tempo real, a polícia pode controlar áreas públicas de forma mais eficiente, identificando incidentes em andamento e possibilitando uma resposta rápida para garantir a segurança pública. Além disso, a integração dos sistemas de videovigilância com outras fontes de dados, como bases de dados de criminalidade, registos de veículos roubados ou informações sobre indivíduos de

interesse, é uma aplicação que fornece informações mais abrangentes e auxilia na identificação de potenciais ameaças.

Por fim, importa referir a tecnologia que trata os dados biométricos, conhecida como reconhecimento facial, não é admissível de ser utilizada, como foi referido ao longo desta dissertação, no entanto, seria uma excelente ferramenta se for enquadrada legalmente, pois possibilita a identificação de suspeitos pela prática de crimes, terroristas já referenciados, ou até mesmo, pessoas desaparecidas. Seria necessário enquadrar de forma a proteger os DLG dos cidadãos e só deveria ser utilizada de forma adequada, proporcional e justa.

Contudo, como já referido anteriormente, é de grande importância a proteção dos dados pessoais e da vida privada, para tal, e para que os seus dados biométricos não fiquem armazenados, a IA pode ser utilizada para tornar impercetível a cara das pessoas, e tapa os locais privados, como por exemplo as residências, para esse efeito são utilizadas as "máscaras". De acordo com o E1, no contexto da videovigilância, as máscaras são técnicas usadas para proteger a privacidade e a identidade das pessoas ou edifícios privados capturados em imagens ou vídeos. Ainda refere o E2 que "uma mascara é uma mancha preta, que impede a visualização e gravação de imagens daquela zona" (E2), ainda acrescenta que essas máscaras podem ser aplicadas digitalmente, ocultando ou desfocando partes específicas do rosto, como olhos, boca ou nariz, ou partes dos edifícios privados como janelas ou portas, com o objetivo de tornar difícil ou impossível para algoritmos de reconhecimento facial identificarem ou rastrearem uma pessoa ou visualizar para dentro de edifícios privados (E2), isso é feito para equilibrar a necessidade de segurança com a proteção da vida privacidade.

CONCLUSÕES E RECOMENDAÇÕES

Através deste estudo, foi possível examinar o ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos, explorar o espectro de aplicações tecnológicas que podem ser utilizadas nesses sistemas e investigar a viabilidade da IA como uma ferramenta potencialmente útil. Compreender os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos revelou-se crucial para a sociedade atual, onde a segurança é uma preocupação constante.

O objetivo geral deste trabalho de investigação foi avaliar os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos. Para alcançar esse objetivo, foram delineados os objetivos específicos de examinar o ordenamento jurídico nacional, explorar as aplicações tecnológicas e investigar a viabilidade da IA.

No que diz respeito ao ordenamento jurídico nacional, constatou-se a existência de regulamentações específicas que estabelecem as condições e limites para a implantação e operação desses sistemas. Essas regulamentações são fundamentais para garantir a proteção dos direitos individuais e a preservação da privacidade dos cidadãos. Através de análises detalhadas das Leis e regulamentos pertinentes, foi possível obter uma compreensão abrangente do quadro jurídico que orienta a videovigilância policial em espaços públicos.

Além disso, a pesquisa explorou o espectro de aplicações tecnológicas disponíveis para esses sistemas, abrangendo os sistemas de monitorização em tempo real e analítica de vídeo, o reconhecimento facial e deteção de comportamentos e objetos suspeitos. Essas tecnologias demonstraram o potencial para aumentar a eficácia e a eficiência da segurança pública, mas também levantaram questões éticas e preocupações relacionadas com o uso adequado dos dados pessoais e à possibilidade de discriminação algorítmica.

A viabilidade da IA nos sistemas de videovigilância policial em espaços públicos foi também investigada, reconhecendo tanto os benefícios quanto os desafios associados. A IA pode aprimorar a deteção de atividades suspeitas e melhorar a capacidade de resposta das forças policiais. No entanto, é essencial abordar questões éticas, garantir a transparência e a prestação de contas, além de evitar a amplificação de vieses e discriminação algorítmica.

Em conclusão, este estudo abordou de forma abrangente os desafios da videovigilância policial em espaços públicos. Ao examinar o ordenamento jurídico nacional, explorar as aplicações tecnológicas e investigar a viabilidade da IA, foi possível compreender as complexidades desse campo e destacar a importância de um equilíbrio entre a segurança pública e a proteção dos direitos individuais. A continuidade desse debate e a

busca por soluções adequadas são essenciais para garantir a segurança da sociedade, mantendo os princípios democráticos e respeitando os direitos civis. Neste enlace, foram detetados alguns desafios para a implementação dos sistemas de videovigilância em espaços públicos. Um desses desafios é o facto de ser necessário o parecer da CNPD, onde é necessário fazer a fundamentação da sua utilização, e incluir ainda todas as especificidades dos equipamentos a serem utilizados, estes pareceres, apesar de não serem vinculativos, devem ser sempre seguidos, de modo a não suscitarem posteriormente duvidas quanto à proteção de dados dos cidadãos os quais lhes foram captadas imagens. Outro desafio apresentado, é a manutenção do equipamento, e a renovação para que os mesmo se mantenha atualizado com a tecnologia de ponta, deste modo é necessário um investimento contínuo, para ser mantida a máxima rentabilidade dos sistemas.

Destaca-se que o grande desafio enfrentado atualmente é encontrar um equilíbrio entre a necessidade de utilizar a tecnologia existente e a proteção da privacidade dos indivíduos. A evolução tecnológica trouxe benefícios significativos para a deteção de crimes e a criação de padrões de comportamentos que inibem a ocorrência de problemas. No entanto, a intrusão na privacidade das pessoas é uma preocupação legítima.

Embora a utilização da tecnologia seja uma vantagem no combate à criminalidade e na promoção da segurança, é importante considerar os aspetos éticos e legais relacionados à privacidade. A proteção de dados pessoais é um direito fundamental que deve ser preservado, mesmo diante das necessidades de segurança pública.

Portanto, o grande desafio é encontrar soluções que permitam o uso eficiente da tecnologia existente, ao mesmo tempo em que se garantem mecanismos adequados de proteção de dados pessoais. É necessário investir em políticas e regulamentações que estabeleçam diretrizes claras sobre o uso e o acesso a informações sensíveis, de forma a conciliar a eficácia na prevenção e combate ao crime com a preservação dos direitos individuais.

Além disso, é importante promover um debate amplo e aberto envolvendo diversos setores da sociedade, incluindo especialistas em tecnologia, legisladores, organizações de defesa dos direitos civis e a população em geral. Somente por meio do diálogo e pela procura de soluções equilibradas será possível enfrentar o desafio de utilizar a tecnologia existente de forma responsável, maximizando seus benefícios e minimizando as suas potenciais vulnerabilidades.

Face ao exposto, é possível responder à pergunta de partida proposta inicialmente. Nesta senda, diversos desafios quanto à aplicação dos sistemas de videovigilância em

espaços públicos foram identificados ao longo desta investigação. Quanto ao quadro jurídico, é necessário cumprir e respeitar o ordenamento jurídico nacional, que estabelece condições e limites para a implantação e operação dos sistemas de videovigilância policial, o que envolve proteger os direitos individuais e preservar a privacidade dos cidadãos. Relativamente às tecnologias e aplicações utilizadas, existe uma ampla gama de tecnologias disponíveis para esses sistemas, como monitorização em tempo real, análise de vídeo, reconhecimento facial e deteção de comportamentos suspeitos, que trazem benefícios para a eficácia da segurança pública, mas também levantam questões éticas e preocupações em relação ao uso adequado dos dados pessoais e à possibilidade de discriminação algorítmica. Mais especificamente, em relação à utilização da IA nos sistemas de videovigilância policial oferece vantagens, como aprimorar a deteção de atividades suspeitas e melhorar a capacidade de resposta das forças policiais. Contudo, é necessário abordar questões éticas, garantir a transparência, evitar vieses e discriminação algorítmica. Outro grande desafio, é garantir a proteção de dados pessoais, captados pelos sistemas de videovigilância policial, especialmente considerando a necessidade de pareceres da CNPD. A utilização adequada e segura desses dados é essencial para evitar quaisquer dúvidas futuras quanto à proteção da privacidade dos cidadãos. Por último, o desafio da manutenção e renovação contínua dos equipamentos de videovigilância policial é crucial para manter a eficácia e a rentabilidade dos sistemas, sendo necessário investimento constante para garantir que os equipamentos estejam atualizados com as últimas tecnologias disponíveis.

Encontrar um equilíbrio adequado entre a necessidade de utilizar a tecnologia existente e proteger a privacidade dos indivíduos é um dos principais desafios enfrentados atualmente. É necessário considerar os aspetos éticos, legais e a proteção de dados pessoais, preservando os direitos fundamentais dos cidadãos.

Esta investigação contribui para um melhor entendimento dos atuais sistemas de videovigilância, e de que forma estão a ser utilizados. Contribui anda para a perceção dos desafios que estão inerentes à aplicação destes sistemas em espaço publico, fazendo um balanço entre a segurança e a proteção dos direitos pessoais.

É de referir que na elaboração desta dissertação foram encontradas diversas limitações, nomeadamente a escassez de especialistas nesta área, e por esse motivo só foi possível contactar e entrevistar quatro entidades com conhecimento e experiência.

Cumpre então referir que o objetivo geral desta investigação foi plenamente atingido ao abordar de maneira abrangente os desafios relacionados à aplicação dos sistemas de videovigilância policial em espaços públicos. Por meio da análise do ordenamento jurídico

nacional, da exploração das aplicações tecnológicas e da investigação da viabilidade da IA nesses sistemas, foi possível obter um entendimento aprofundado das complexidades e questões éticas envolvidas. Assim, este estudo cumpriu seu objetivo de avaliar e compreender os desafios inerentes à videovigilância policial em espaços públicos.

Para futuras investigações sugere-se realizar estudos com forças de segurança internacionais congéneres às portuguesas, de forma a serem conhecidos os seus sistemas de videovigilância, e de que forma podem ser aplicados no contexto português, de acordo com a legislação em vigor. Sugere-se ainda que seja feito um estudo sobre a evolução da criminalidade, antes e após a utilização de sistemas de videovigilância polícia, em que a IA seja utilizada. Não obstante, dado a relevância e impacto da IA na sociedade atual, importa que, futuramente, se desenvolvam também estudos sobre a sua aplicação enquanto ferramenta de proteção dos DLG, em especial na utilização de sistemas de videovigilância policial.

BIBLIOGRAFIA

Albuquerque, S. I. S. (2022). *O impacto da tecnologia no policiamento*. Trabalho de Investigação Individulal, Instituto Universitário Militar, Lisboa.

Alves, R., A., V. (2018). *Emprego de meios tecnológicos na vigilância florestal em Portugal*. Trabalho de Investigação Individual, Instituto Universitário Militar, Lisboa

Arroyo, R., Yebes, J. J., Bergasa, L. M., Daza, I. G., & Almazán, J. (2015). Expert video-surveillance system for real-time detection of suspicious behaviors in shopping malls. *Expert Systems with Applications*, *42*(21), 7991–8005. https://doi.org/10.1016/j.eswa.2015.06.016.

Bruno, F. (2012). Contra-Manual Para Câmeras Inteligentes: Vigilância, Tecnologia e Percepção. *Galáxia*, *12*(24), 47–63.

Comissão Europeia (2018). *Inteligência artificial para a Europa*. Acedido em 20/03/2023 em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=COM%3A2018%3A237%3AFIN.

Comissão Europeia (2020). *Livro branco sobre a inteligência artificial — Uma abordagem europeia virada para a excelência e a confiança*. Acedido 24/03/2023 em https://op.europa.eu/pt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1

Correia, E. P. & Duque, R. S. (2012). *O Poder Político e a Segurança.* Lisboa: Fonte da Palavra.

Costa, I. S. (2021). A proteção da pessoa na era dos big data: a opacidade do algoritmo e as decisões automatizadas. *Revista Electrónica de Direito*, *24*(1), 33–82. https://doi.org/10.24840/2182-9845_2021-0001_0004

COTEC/ADAI (2005). *Incêndios Florestais Estudo sobre sistemas de Vigilância de Incêndios Florestais*. Lisboa: COTEC.

Coutinho, C. (2013). *Metodologia de Investigação em Ciências Sociais e Humanas: Teoria e Prática* (2ª Ed.). Coimbra: Almedina.

Creswell, J. W. (2009). Research design: Qualitative, quantitative, and mixed methods approaches. In *Intercultural Education* (Vol. 20, Issue 2). https://doi.org/10.1080/14675980902922143.

Creswell, J. W. (2018). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches*. SAGE Publications.

Denzin, N. K., & Lincoln, Y. S. (2003). Introduction: The discipline and practice of

qualitative research. *Collecting and interpreting qualitative materials* (pp. 1-45). Thousand Oaks, CA: Sage Publications.

Domingos, P. (2012). A Few Useful Things to Know About Machine Learning. *Communications of the ACM*, *55*(10), 79–88.

Domingos, P. (2017). A revolução do algoritmo mestre. Barcarena: Manuscrito.

Durães, D. F. M. (2008). *Arquitectura de sistema de vigilância integrada*. Dissertação de Mestrado, Faculdade de Engenharia da Universidade do Porto, Porto.

Eco, U. (2007). *Como se Faz uma Tese em Ciências Humanas*. Lisboa: Editorial Presença.

Floridi, L., Cowls, J., Belltrametti, M., Chatila, R., Chazerand,P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P. & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. *Minds and Machines* 28, 689-707. https://doi.org/10.1007/s11023-018-9482-5

Fortin, M.-F. (1999). *O Processo de Investigação: Da concepção à realização*. (N. Salgueiro, Trad.) Loures: Lusociência.

Fortin, M.-F. (2009). *O Processo de Investigação: Da Conceção à Realização* (5.ª ed.). Loures: Lusociência.

Frąckiewicz, M. (2023). *O papel da IA na segurança cibernética e na proteção de dados* [Página online]. Acedido em 15/05/2023 em https://ts2.space/pt/o-papel-da-ia-na-seguranca-cibernetica-e-na-protecao-de-dados/.

GNR (2022). Comunicado: Reforço da vigilância da GNR no incêndio da Serra da Estrela. Acedido em 15/05/2023 em https://www.gnr.pt/comunicado.aspx?linha=4751.

Hanmann, K., & Smith, R. (2018). Face Recognition Technology. *International Journal of Trend in Scientific Research and Development*. 2 (4), 1612–1613. https://doi.org/10.31142/ijtsrd14331.

Hert, P. & Papakonstantinou, V., (2011). The Proposed Data Protection Regulation Replacing Directive 95/46/Ec: A Sound System for the Protection of Individuals (2011). *Computer Law & Security Review*. 28(2), 130–142.

Information Comissioner's Office (2017). *Big data, artificial intelligence, machine learning and data protection.* Acedido em 16/05/2023 em https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

InternationlIT (2023). Inteligência Artificial (IA): Detecção de Anomalias de Rede e Combate ao Ransomware. Acedido em 19/05/2023 em https://www.internationalit.com/post/intelig%C3%AAncia-artificial-ia-

detec%C3%A7%C3%A3o-de-anomalias-de-rede-e-combate-ao-ransomware.

Kissinger, H., Schmidt, E. & Huttenlocher, D. (2021). *A era da inteligência artificial* (1.ª Edição). Alfragide: Dom Quixote

Lakatos, E., & Marconi, M. (2003). *Fundamentos de metodologia científica* (5.ª ed.). São Paulo: Editora Atlas.

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

Moleirinho, P. M. S. E. (2021). *Aplicação da inteligência artificial ao serviço da função policial*. Trabalho de Investigação Individual, Instituto Universitário Militar, Lisboa.

Monte, M. (2013). Direito Penal da Sustentabilidade? Tópicos para um novo paradigma na tutela penal do ambiente. *Jurismat*, (3), 91-101.

Morgan, F., Boudreaux, B., Lohn, A., Ashby, M., Curriden, C., Klima, K., Grossman, D. (2020). *Military Applications of Artificial Intelligence - Ethical Concerns in an Uncertain World*. California: Rand Corporation. Acedido em 16/04/2023 em https://www.rand.org/pubs/research_reports/RR3139-1.html.

Nabeel, F. (2019). *Regulating facial recognition technology in public places.* Centre for Strategic and Contemporary Research. Acedido em 15/05/2023 em https://www.academia.edu/39871139/Regulating_Facial_Recognition_Technology_in_Public_Places.

Neves, P., & Guerra, R. (2015). *Teses em Ciências Sociais - Dicas Muito Práticas*. Lisboa: Edições Sílabo.

Nunes, M. C. de P. T. P. (2011). *Videovigilância da Prevenção à Repressão Questões de violação da privacidade e valia probatória*. Dissertação, Mestrado Forense, Universidade Católica Portuguesa, Lisboa.

Parlamento Europeu. (2021a). *O que é a Inteligência Artificial e como funciona?*. Acedido em 10/02/2023 https://www.europarl.europa.eu/news/pt/headlines/society/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona.

Parlamento Europeu (2021b). *Draft report on artificial intelligence in a digital age.* Special Committee on Artificial Intelligence in a Digital Age. 2020/2266(INI).

Pardal, L. & Correia, E. (1995). *Métodos e Técnicas de Investigação Social*. Lisboa: Areal Editores.

Pereira, D. J. R. (2019). *O sistema de videovigilância — Prevenção e investigação criminais*.

Dissertação de Mestrado, Universidade Nova de Lisboa, Lisboa.

Pereira, L. A. S. P. (2017). *Políticas de segurança e a videovigilância urbana - o caso da Amadora*. Trabalho de Investigação Final, Instituto Superior de Ciências Policias e Segurança Interna, Lisboa

Police Transparency Unit (2013). *Surveillance Camera Code of Practice.* London: The Stationery Office.

Prodanov, C., & Freitas, E. (2013). *Metodologia do Trabalho Científico: Métodos e Técnicas da Pesquisa e do Trabalho Acadêmico*. Novo Hamburgo: Universidade Feevale.

Quivy, R., & Campenhoudt, L. (2005). *Manual de investigação em ciências sociais* (4.ª Ed.). Lisboa: Gradiva.

Renda, A. I., Ribeiro, F. P., & Baleiro, R. (2017). *Manual de regras para trabalhos académicos em ciências sociais: organizar, escrever e formatar*. Lisboa: Edições Colibri.

Rodrigues, L. F. (2022). Direitos humanos e a era digital: a necessidade da proteção de dados como um direito fundamental. *Revista ratio iuris.*1(1), 279-299. Acedido em 26/04/2023 em https://periodicos.ufpb.br/index.php/rri/article/view/63385.

Rosado, D. P. (2015). *Sociologia da Gestão e das Organizações*. Lisboa: Gradiva.

Santos, L. A., Lima, J. M., Garcia, F. M., Monteiro, F. T., Silva, N. M., Silva, J. C., & Santos, R. J. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (2.ª edição). Lisboa: Instituto de Estudos Superiores Militares

Sarmento, M. (2013). *Metodologia científica para a elaboração, escrita e apresentação de teses*. Lisboa: Universidade Lusíada Editora.

Security Magazine (2021). *Uma Nova Era para a Analítica de Vídeo*. Acedido em 28/03/2023 em https://www.securitymagazine.pt/2021/12/08/uma-nova-era-para-a-analitica-de-video/.

Segurança Eletrónica (2022). *O que é Vídeo Analítico e como ele funciona*. [Página online]. Acedido em 20/05/23 em https://revistasegurancaeletronica.com.br/o-que-e-video-analitico-e-como-ele-funciona/.

Porto Editora – *videovigilância* no Dicionário infopédia da Língua Portuguesa. Porto: Porto Editora. Acedido em 20/02/2023 em https://www.infopedia.pt/dicionarios/lingua-portuguesa/videovigilância

Sistema de Segurança Interna [SSI] (2023). *Relatório Anual de Segurança Interna - Ano 2022*. Lisboa: SSI.

Strauss, A., & Corbin, J. (1998). *Basics of qualitative research: Techniques and rocedures*

for developing grounded theory. London: Sage Publications.

Veiga, A. S. P. G. (2020). *Proteção de dados: o direito à privacidade na era digital*. Dissertação de Mestrado, Mestrado em Direito, Universidade Autónoma de Lisboa, Lisboa.

Vygotsky, L., & Cole, M. (2018). Lev Vygotsky: Learning and social constructivism. Learning theories for early years practice, 66, 58.

Vu, B., (2018). *A Technological and Ethical Analysis of Facial Recognition in the Modern Era*. California: The University of California.

Legislação

Assembleia Geral da ONU. (1948). Declaração Universal dos Direitos Humanos. Resolução 217 [III] A. Paris.

Assembleia Geral das Nações Unidas (1966). Pacto Internacional sobre os Direitos Civis e Políticos. 2200-A (XXI). Nova Iorque. Acedido em 15/02/2023 em https://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf

Conselho da Europa (1950). Convenção Europeia dos Direitos do Homem. Acedido em 15/02/2023 em https://www.echr.coe.int/documents/convention_por.pdf

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

Decreto-lei n.º 47344/66, de 25 de novembro (1966). Código Civil. Diário do Governo n.º 274/1966, Série I de 1966-11-25. Lisboa: Governo.

Lei n.º 1/1976, de 10 de abril (1976). *Constituição da República Portuguesa. Diário da República* n.º 86/1976, 1ª Série, 86, 738-775. Lisboa: Assembleia da República.

Lei n.º 49/2008, de 27 de agosto (2008). *Lei de Organização da Investigação Criminal.* Diário da República, 1ª série, 165. Lisboa: Assembleia da República.

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

Lei n.º 58/2019, de 8 de agosto (2019ª). *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 n.º 151, 1ª série, 3-40.

Lisboa: Assembleia da República.

Lei n.º 59/2019, de 8 de agosto (2019b). *Aprova as regras relativas ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais, transpondo a Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.* Diário da República n.º 151, 1ª série, 41-68. Lisboa: Assembleia da República.

Lei n.º 95/2021, de 29 de dezembro (2021). *Regula a utilização e o acesso pelas forças e serviços de segurança e pela Autoridade Nacional de Emergência e Proteção Civil a sistemas de videovigilância para captação, gravação e tratamento de imagem e som, revogando a Lei n.º 1/2005, de 10 de janeiro*. Diário da República n.º 251, 1.ª série,3-12. Lisboa: Assembleia da República.

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Regulamento Geral sobre a Proteção de Dados. Jornal Oficial da União Europeia, L 119/1. Bruxelas: UE.

União Europeia (2000). Carta dos Direitos Fundamentais da União Europeia. Jornal Oficial da União Europeia, C 202/389

APÊNDICES

Apêndice A - Modelo de Análise

Tabela 4- Modelo de Análise

Tema: Os desafios da videovigilância policial em espaços públicos	
Pergunta de partida: Quais os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos?	
Objeto de estudo: Aplicações tecnológicas nos sistemas de videovigilância policial.	
Objetivo Geral: Avaliar os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos.	
OE1: Analisar o ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos.	**Cap I**
PD1: Qual o ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos?	
OE2: Analisar o espectro de aplicações tecnológicas que podem ser utilizadas em sistemas de videovigilância policial em espaços públicos.	**Cap II**
PD2: Que aplicações tecnológicas podem ser admissíveis nos sistemas de videovigilância policial em espaços públicos?	
OE3: Investigar a aplicabilidade da Inteligência Artificial nos sistemas de videovigilância policial em espaços públicos.	**Cap III**
PD3: Que aplicabilidade tem a Inteligência Artificial nos sistemas de videovigilância policial em espaços públicos?	

Fonte: Elaboração Própria

Apêndice B - Carta de Apresentação

ACADEMIA MILITAR

Os desafios da videovigilância policial em espaços públicos

Autor: Aspirante de GNR Infantaria Gonçalo Tibério Faria

Orientador: Tenente-Coronel de Infantaria Renato Pessoa dos Santos

Coorientador: Major Gonçalo Nuno Correia Zambujo Serrão

Mestrado Integrado de Ciências Militares na Especialidade de Segurança

Relatório Científico Final do Trabalho de Investigação Aplicada

Lisboa, maio de 2023

CARTA DE APRESENTAÇÃO

A missão da Academia Militar é capacitar e formar Oficiais dos quadros permanentes do Exército e a Guarda Nacional Republicana (GNR). No curso de Ciências Militares, especialidade em Segurança, os alunos devem realizar um Trabalho de Investigação Aplicada (TIA) sobre temas relevantes para a GNR, com o objetivo de obter o grau de Mestre no curso.

Neste contexto, eu, Gonçalo Tibério Faria, Aspirante a Oficial da GNR e a frequentar o 5º e último ano do ciclo de estudo, venho por este meio solicitar a colaboração de V. Ex.ª mediante a participação num inquérito por entrevista com o intuito de recolher informações para o TIA cujo tema é: "Os desafios da videovigilância policial em espaços públicos".

A presente investigação destina-se a caracterizar os sistemas de videovigilância policial e tem como objetivo propor aplicações tecnológicas passíveis de implementação nos sistemas de videovigilância da GNR em espaços públicos, em cumprimento do ordenamento jurídico vigente. Por conseguinte, torna-se imprescindível recolher dados e captar a experiência dos profissionais da GNR que lidam com a videovigilância.

Desta forma, apraz-me solicitar o consentimento de Vossa Excelência para responder à referida entrevista, bem como para autorizar a respetiva gravação para posterior tratamento e análise da informação. A entrevista terá uma duração sensivelmente de 30 minutos e, caso pretenda, no final ser-lhe-á concedida a transcrição da mesma.

Assim sendo, apraz-me solicitar a sua autorização para realizar a entrevista mencionada, e para gravá-la com o intuito de posteriormente analisar e tratar a informação obtida. A duração estimada da entrevista é de cerca de 30 minutos e, se desejar, ser-lhe-á fornecida a transcrição completa da mesma no final.

A sua colaboração é fundamental para alcançar os objetivos desta investigação. Assim, agradeço antecipadamente pela sua disponibilidade e atenção.

Muito respeitosamente,
Gonçalo Tibério Faria
Aspirante de Infantaria da GNR

Apêndice C - Guião de Entrevista

GUIÃO DA ENTREVISTA

- Toda a informação recolhida nesta entrevista será apenas utilizada no Trabalho de Investigação Aplicada.
- Se assim o entender, e para que não se perca informação, a entrevista será gravada.
- Sendo uma entrevista algo dinâmico, para além das perguntas a seguir estipuladas, poderão ocorrer outras perguntas que no nosso entender serão relevantes para a investigação.

1. IDENTIFICAÇÃO DO ENTREVISTADO

Nome:

Idade:

Cargo/Posto:

Função:

Local:

Data:

Hora de início;

Hora do fim:

2. GUIÃO DE ENTREVISTA

Pergunta 1 - Qual a legislação em vigor que regula a utilização de sistemas de videovigilância policial em espaços públicos pelas Forças de Segurança?

Pergunta 2 - Quais as principais exigências legais para a implementação dos sistemas de videovigilância policial em espaços públicos?

Pergunta 3 - Quais as lacunas que identifica no ordenamento jurídico em vigor que regula a utilização de sistemas de videovigilância policial?

Pergunta 4 - Quais os pontos fortes e fracos do ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos?

Pergunta 5 - Que tipo de aplicações tecnológicas podem e devem ser aplicadas nos sistemas de videovigilância policial em espaços públicos?

Pergunta 6 - Com a evolução da tecnologia e a implementação da Inteligência Artificial em diversos setores, de que forma poderá esta ser utilizada nos sistemas de videovigilância policial, de acordo com o ordenamento jurídico em vigor?

Pergunta 7 - No domínio do tratamento e análise de dados, quais as especificações técnicas dos equipamentos de videovigilância que poderão afetar a privacidade das pessoas, em particular os seus Direitos, Liberdades e Garantias, e de que forma poderá este problema ser impedido?

Pergunta 8 - Quais as Vantagens/oportunidades podem ser apontadas à utilização dos sistemas de videovigilância com IA?

Pergunta 9 - Quais as desvantagens/ameaças podem ser apontadas à utilização dos sistemas de videovigilância com IA?

Apêndice D - Consentimento Informado

Consentimento Informado

Tenho conhecimento que um investigador da Academia Militar está a realizar um estudo que pretende apurar "Os desafios do avanço tecnológico dos sistemas de videovigilância policial em espaços públicos". O estudo tem como investigador o Aspirante Gonçalo Tibério Faria, com a orientação do Tenente-Coronel Renato Pessoa dos Santos (Academia Militar) e do Major Gonçalo Nuno Correia Zambujo Serrão (Comando-Geral GNR).

Se concordar participar, vou ser entrevistado individualmente pelo Aspirante Gonçalo Tibério Faria, onde iremos debater ideias acerca desta temática. A entrevista tem uma duração média entre 30 e 45 minutos e será gravada em áudio, mas ninguém saberá aquilo que eu disser na entrevista, à exceção das pessoas da que estão a fazer este estudo. Eu tenho o direito de responder apenas às perguntas que quiser. Compreendo que posso não ganhar nada diretamente por participar neste estudo, mas a minha participação poderá ser muito útil para outras pessoas, no futuro. No final do estudo poderei ter acesso aos resultados do mesmo, através da solicitação ao investigador.

Aceito participar neste estudo e aceito ser entrevistado(a) no dia _____, pelas _____ horas. Se, em algum momento, decidir que não quero participar, posso desistir e não preciso de explicar as minhas razões e isso não terá nenhumas consequências negativas para mim.

Assinatura: _____

Data: ____/____/_____

Muito obrigado pela colaboração.

Pelo investigador,

_____

_____

Para qualquer esclarecimento, contactar faria.gt@gnr.pt

Apêndice E - Relação entre pergunta derivadas e questões da entrevista

TEMA		**Os desafios da videovigilância policial em espaços públicos**
Objetivo Geral		Avaliar os desafios inerentes à aplicação dos sistemas de videovigilância policial em espaços públicos.
Objetivo de estudo		Aplicações tecnológicas nos sistemas de videovigilância policial.
Objetivos específicos		
OE1	Analisar o ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos	P1 - Qual a legislação em vigor que regula a utilização de sistemas de videovigilância policial em espaços públicos pelas Forças de Segurança? P2 - Quais as principais exigências legais para a implementação dos sistemas de videovigilância policial em espaços públicos? P3 - Quais as lacunas que identifica no ordenamento jurídico em vigor que regula a utilização de sistemas de videovigilância policial? P4 - Quais os pontos fortes e fracos do ordenamento jurídico nacional aplicável aos sistemas de videovigilância policial em espaços públicos?
OE2	Analisar o espectro de aplicações tecnológicas que podem ser utilizadas em sistemas de videovigilância policial em espaços públicos	P5 - Que tipo de aplicações tecnológicas podem e devem ser aplicadas nos sistemas de videovigilância policial em espaços públicos? P6 - No domínio do tratamento e análise de dados, quais as especificações técnicas dos equipamentos de videovigilância que poderão afetar a privacidade das pessoas, em particular os seus Direitos, Liberdades e Garantias, e de que forma poderá este problema ser impedido?
OE3	Investigar a aplicabilidade da Inteligência Artificial nos sistemas de videovigilância	P7 -Com a evolução da tecnologia e a implementação da Inteligência Artificial em diversos setores, de que forma poderá esta ser utilizada nos sistemas de videovigilância policial, de acordo com o ordenamento jurídico em vigor? P8 -Quais as Vantagens/oportunidades podem ser apontadas à utilização dos sistemas de videovigilância com IA? P9 -Quais as desvantagens/ameaças podem ser apontadas à utilização dos sistemas de videovigilância com IA?

	policial em espaços públicos	