Instituto **S**uperior de **C**iências **P**oliciais e **S**egurança **I**nterna

A INTELIGÊNCIA ARTIFICIAL NA VIDEOVIGILÂNCIA – BENEFÍCIOS E RISCOS ASSOCIADOS - O PAPEL DA PSP NO CONTROLO DO SISTEMA

Autor: Vítor Miguel Ferreira da Silva

Estudo Teórico

Trabalho Final do 5.º Curso de Comando e Direção Policial

Lisboa, 20 de fevereiro de 2023

Resumo

O desenvolvimento tecnológico abrupto da Inteligência Artificial tem criado impacto nas nossas vidas e numa economia fortemente impulsionada pelos dados. Compete aos Governos enfrentar esta nova realidade com ações construtivas concretas que garantam uma regulamentação equilibrada e eficaz, encontrando um ponto de equilíbrio entre a proteção dos cidadãos e, por outro lado, o incentivo à inovação e competitividade que nos permita beneficiar das enormes potencialidades do progresso tecnológico. A aplicação de sistemas de Inteligência Artificial no apoio à atividade policial é algo pouco comum e regulamentado. Na senda, o objetivo deste estudo foi perceber se os vários normativos nacionais em vigor relativos à utilização de sistemas de Inteligência Artificial na videovigilância se encontram em harmonia com as diretrizes da União Europeia e se poderá haver uma maximização das potencialidades desta ferramenta não pondo em causa direitos, liberdades e garantias. Concluímos que a legislação portuguesa está desadequada necessitando de uma restruturação que obrigará à criação de uma Autoridade Nacional de Controlo e a atribuição de competências de fiscalização a autoridades já existentes nos vários setores da sociedade, na qual poderemos destacar a Polícia de Segurança Pública para supervisão de sistemas de videovigilância com Inteligência Artificial.

Palavras-chave: Inteligência Artificial; Polícia; Regime Jurídico; Videovigilância.

Abstract

Artificial intelligence's abrupt technological development has impacted our lives in an economy strongly driven by data. It is the government's responsibility to face this new reality with concrete and constructive actions that guarantee stable and effective regulation, balancing the protection of citizens with innovation and competitiveness encouragement that will allow all of society to benefit from the progress and enormous technological potential. The application of artificial intelligence systems in support of police activity is uncommon and regulated. With this, the goal of this research is to determine whether force national regulations governing the use of artificial intelligence systems in video surveillance are consistent with European Union guidelines. In addition, we also checked the potential use maximization of this tool without jeopardizing rights, freedoms, and guarantees. We conclude that the Portuguese legislation is insufficient, necessitating a reorganization that calls for the establishment of a national control authority as well as the delegation of supervisory powers to existing squads in various sectors of society, highlighting the Public Security Police for the supervision of video surveillance systems with artificial intelligence.

Keywords: Artificial intelligence; Police; Legal System; Video surveillance

Introdução

Estamos marcados por uma era tecnológica num mundo onde se verifica o impacto e dependência da tecnologia nas pessoas, empresas e sociedade no geral, sob a forma de máquinas, sensores, câmaras ou algoritmos que geram dados e moldam comportamentos (Veiga, 2021). Com a "globalização, deslocamentos e mudanças aceleradas, as grandes cidades transformaram-se em expressões concentradas e intensificadas dos problemas sociais que afetam a sociedade como um todo", podendo assim gerar conflitos violentos (Giddens, 2005, p.463).

Atualmente a sociedade exige que o Estado assuma um papel proativo no combate ao crime e (ao) sentimento de insegurança, exigindo "respostas políticas interdisciplinares e multifacetadas, porque, (…) a segurança é fundamentalmente uma questão política" (Oliveira, 2006, p.81). Neste pressuposto, os governos começaram a adotar um papel preponderante para colmatar esta necessidade desenvolvendo programas especiais de policiamento de proximidade e envolvimento de parceiros numa intervenção superior dos Conselhos Municipais de Segurança. Assumindo esse desígnio, as autarquias envolveram-se nos contratos-programa de policiamentos de proximidade e instalação de dispositivos de prevenção como os sistemas de Videovigilância – *Closed Circuit Television* (CCTV) (Pereira, 2017).

No entanto, os sistemas de CCTV, tal como os conhecíamos, estão praticamente obsoletos dada a evolução que a Inteligência Artificial (IA) tem adquirido nos últimos anos e a implementação destas ferramentas digitais nos circuitos de CCTV. A Comissão Europeia (CE) (2018) refere que as economias mais desenvolvidas, como os Estados Unidos da América com o investimento de cerca de 970 milhões de euros em investigação na área da IA e a China que pretende alcançar a liderança económica global até 2030, com a criação de um parque tecnológico dedicado à IA, no valor de 1 700 milhões de euros, em Pequim (Comissão Europeia, 2018), estão cientes da revolução que se avizinha com a implementação da IA com implicações nos sistemas políticos, económicos, culturais e sociais. Paralelo a esta problemática, está o desinvestimento privado Europeu que em 2016 apenas existiu um investimento de cerca de 3 200 milhões de euros sendo este um valor bastante abaixo em comparação com investimentos de 9 700 milhões de euros na Ásia ou 18 600 milhões de euros na América do Norte (Comissão Europeia, 2018).

Desta forma, é crucial que a União Europeia (UE) crie condições favoráveis ao desenvolvimento coordenado da IA nos países membros fomentando o investimento público e privado neste sector com a disponibilização de fundos europeus para ambos e

desenvolvendo vários regulamentos de controlo (Comissão Europeia, 2018). A UE publicou em 2020 o "Livro Branco sobre a inteligência artificial" (Comissão Europeia, 2020b) onde refere que a IA também pode ser utilizada no garante da segurança dos cidadãos. Em Portugal criou-se o documento "IA Portugal 2030" como estratégia para a construção de um mercado económico mais tecnológico e competitivo destacando o foco apenas nos setores da educação, saúde, agricultura e indústria, deixando de parte o investimento público no setor da segurança interna e externa (Fundação para a Ciência e Tecnologia, 2021).

Em 26 de janeiro do presente ano, o jornal de negócios publicou um artigo onde refere que o Governo português disponibilizou 77 milhões de euros do Plano de Recuperação e Resiliência para as duas principais empresas portuguesas de desenvolvimento da IA em Portugal: a Defined.ai e a Unbabel. No mesmo artigo e, em entrevista à CEO da Defined.ai, Daniela Braga refere que este investimento coloca Portugal num patamar de destaque na Europa e que muitos dos países membros desistiram do investimento nesta temática (Velho, 2023).

É notório o investimento Europeu focado na IA na tentativa de colocar a Europa no topo da economia mundial. Portugal tem demonstrado preocupação e investimento nesta matéria apesar de não se prever um investimento público direto em tecnologia de apoio à segurança interna.

O impacto desta temática na atividade policial é de grande contributo, por já nos encontrarmos a monitorizar sistemas de videovigilância com algumas aplicações de IA que nos ajudam a direcionar o policiamento e os meios humanos de forma mais eficaz, havendo ainda a necessidade de perceber os limites para a aplicação de sistemas de IA pela possibilidade dos dados gerados serem confundidos com dados pessoais ou se por outro lado, podemos evoluir até à máxima potencialidade do sistema. Atualmente, já nos encontramos a fiscalizar sistemas de videovigilância no setor privado com IA incorporada.

Estado de Arte

Contextualização teórica

A prevenção criminal

Compete ao poder político criar as condições necessárias para a segurança dos seus cidadãos e para a sua efetivação surgem várias instituições públicas que detêm autoridade em nome do Estado e que usam força e violência de forma concertada e legítima para a garantia da segurança (Oliveira, 2006). A segurança, na sua perspetiva interna, está

consagrada e definida na Lei n.º 53/2008, de 29 de agosto, e em concreto na alínea n.º1 do artigo n.º1 como sendo:

> a atividade desenvolvida pelo Estado para garantir a ordem, a segurança, e a tranquilidade públicas, proteger pessoas e bens, prevenir e reprimir a criminalidade e contribuir para assegurar o normal funcionamento das instituições democráticas, o regular exercício dos direitos, liberdades e garantias fundamentais dos cidadãos e o respeito pela legalidade democrática.

Desta forma, a atribuição da Segurança Interna (SI) às Forças de Segurança (FS) encontra-se moldada na Constituição da República Portuguesa (CRP), no seu artigo 272º onde no n.º 1 refere que "A polícia tem como funções defender a legalidade democrática e garantir a segurança interna e os direitos dos cidadãos". A atribuição de segurança à Polícia de Segurança Pública (PSP) vem considerada na Lei Orgânica da PSP (LOPSP), aprovada pela Lei n.º 53/2007, de 31 de agosto, no seu artigo 1º que refere "A PSP tem por missão assegurar a legalidade democrática, garantir a segurança interna e os direitos dos cidadãos, nos termos da constituição e da lei.".

Através da confluência destes conceitos normativos, o Estado garante a necessidade coletiva de segurança, considerada um bem supra individual, de benefício e interesse público "inato a uma comunidade democraticamente organizada, e por representar a face da cedência dos cidadãos ao poder político de uma das tarefas em troca de uma limitação estreita da liberdade" (Valente, 2014, p.113). Oliveira (2006) acrescenta ainda que a segurança é "uma atividade essencial num Estado de Direito Democrático, levada a cabo por instituições públicas no sentido de garantirem a efetividade dos diretos civis, políticos e sociais" (Oliveira, 2006, p.54). Não basta restabelecer a ordem e segurança pública quando esta é colocada em causa competindo ao Estado "ser dinamizador das condições para a manutenção da tranquilidade pública, prevenindo os problemas, agindo de forma proactiva junto da comunidade e dos cidadãos, de forma a encontrar as soluções para obstar a que fenómenos de desordem se repitam" (Oliveira, 2006, p.17).

Existem dois métodos interventivos como garantia da segurança: métodos repressivos e métodos preventivos. No quadro da SI, a prevenção criminal é apresentada como um dos quatro pilares da dimensão da segurança, sendo as restantes três representadas pela ordem pública (repressão), informações e investigação criminal (Cabral, 2011; Oliveira, 2006). A atuação das FS ao nível da prevenção criminal é essencial para

um combate eficaz da criminalidade (Cabral, 2011). Prevenir de forma eficiente a produção, expansão ou generalização de danos sociais sem que a sociedade se aperceba é a melhor conduta policial (Ferreira, 2005). Segundo Oliveira (2006) alguns tipos de delitos podem ser evitados se tivermos mecanismos de controlo dos espaços e dos ambientes onde eles se geram ou onde existam fortes probabilidades de tal vir a acontecer. A prevenção situacional compreende medidas de dissuasão como o urbanismo, a tecnologia, a vigilância e a videovigilância. Moleirinho (2018) acrescenta que a prevenção exige análises preditivas que requerem a identificação de padrões, para antecipar riscos, informando a ação do decisor. No acompanhamento destes fenómenos criminais e sociais, as FS tem vindo a implementar sistemas de CCTV em locais públicos, para apoio à atividade de prevenção e investigação criminal (Pereira, 2017) e por se afigurar indispensável para a salvaguarda de bens jurídicos superiores, em locais de existência de riscos objetivos (Valente, 2014).

Os Sistemas de CCTV

Frois (2011) cita Dr. Rui Pereira o qual em 2007, enquanto Ministro da Administração Interna, referiu que as sociedades atuais e globais são por natureza sociedades de risco onde os perigos adquirem novas dimensões. Estes quadros de ameaças exigem uma estratégia de resposta inovadora aproveitando as novas tecnologias, em particular os meios de CCTV que "à semelhança do que sucede nos restantes Estados da União Europeia, é também um instrumento fundamental para a prevenção de crimes – e, em particular, de crimes cometidos na via pública" (p.148).

Os sistemas de CCTV estão cada vez mais presentes na nossa vida sendo uma tecnologia multifuncional que poderá ser encontrada na esfera do domínio público e privado. O seu principal uso está relacionado com a gestão de riscos: fluxo de trânsito rodoviário, deteção de incêndios, acidentes e crime, sendo considerada uma tecnologia para detetar riscos, sendo por si só uma tecnologia de risco (Hempel & Topfer, 2002).

As definições mais tradicionais referem os sistemas de CCTV como circuitos fechados compostos por câmaras de vídeo que transmitem imagens para um monitor central e/ou gravadas (Ratcliffe, 2006). Estes sistemas podem ser divididos em dois tipos: o sistema passivo onde "existe um dispositivo de gravação de imagens, em que estas podem ser repetidas posteriormente de um crime é relatado, embora ninguém monitoriza ativamente as imagens", e o sistema ativo onde "uma pessoa monitoriza uma série de ecrãs com imagens em tempo real". Muitos destes apresentam características mistas "onde os dispositivos de gravação gravam todas as imagens, e um operador observa cada monitor,

concentrando-se nuns e ignorando outros" (Ratcliffe, 2006, p.4). Nos últimos anos, a evolução dos sistemas de CCTV tem possibilitado a conjugação das imagens recolhidas pelas câmaras com a capacidade de as analisar e criar um tipo de ação ou alerta, exponenciando intervenções de segurança (Security Magazine, 2021).

A Inteligência artificial nos sistemas de CCTV

A expressão "Inteligência Artificial" foi criada por John McCarthy, em 1956, quando a caracterizou como sendo a engenharia de criar máquinas inteligentes através de processos de engenharia específicos (Spicer, 2007). Durante pouco mais de uma década, existiu investimento público por estar a ser bastante promissor para a investigação. Por questões políticas, em 1973, o Governo Americano e Britânico, os maiores investidores na investigação de IA, suspenderam as suas verbas dando início ao "inverno da Inteligência Artificial" (Haenlein & Kaplan, 2019). Só mais tarde, em 1997, a empresa IMB conseguiu relançar a IA para a ribalta quando o seu programa de xadrez *Deep Blue* conseguiu vencer o campeão do mundo Gary Kasparov através do processamento de 200 milhões de ações possíveis por segundo para calcular a melhor jogada, sendo este o grande passo para a evolução da IA no mundo (Haenlein & Kaplan, 2019). Mais tarde, em 2012, a Google criou os primeiros algoritmos de *deep learning* que identificava gatos através de um conjunto de imagens com a criação de uma rede neuronal com cerca de 16 mil processadores e de mil milhões de conexões, e através da visualização de imagens do youtube, criando uma definição de gato de forma autónoma (Dean, 2012). No mesmo ano a Google desenvolveu a *Alpha Go*, uma rede neuronal artificial que venceu o campeão do mundo no jogo de tabuleiro chines, Ke Lie, um jogo mais complexo que o xadrez (Haenlein & Kaplan, 2019). A grande diferença entre as duas redes é que o Alpha Go baseia-se num novo conceito de *deep learning* (Lee, 2018).

Não existe consensualidade da adoção de um conceito de IA capaz de caracterizar uma tecnologia em constante evolução e mutação, existindo apenas princípios e valores teóricos que tem bases fundamentadas (Wang, 2019) como a autonomia, capacidade de resolução de problemas, possibilidade de raciocínio, da tomada de decisão, previsão, aprendizagem com a experiência, adaptação, reconhecimento visual e auditivo e reconhecimento de objetos (Fundação para a Ciência e Tecnologia, 2021). A IA não se limita a entender situações, mas também escolhe e raciocina, pertencendo à família de tecnologias de rápida evolução (Comissão Europeia, 2021).

Na procura de uma definição generalista para a IA, o Grupo de Peritos de Alto Nível criado pela UE caracterizou-a como os,

> sistemas de software (e eventualmente também de hardware) concebidos por seres humanos, que, tendo recebido um objetivo complexo, atuam na dimensão física ou digital percecionando o seu ambiente mediante a aquisição de dados, interpretando os dados estruturados ou não estruturados recolhidos, raciocinando sobre o conhecimento ou processando as informações resultantes desses dados e decidindo as melhores ações a adotar para atingir o objetivo estabelecido. Os sistemas de IA podem utilizar regras simbólicas ou aprender um modelo numérico, bem como adaptar o seu comportamento mediante uma análise do modo como o ambiente foi afetado pelas suas ações anteriores (Comissão Europeia, 2020b, p.18).

Nos sistemas de IA existem dois elementos essenciais: sensores e algoritmos. Os sensores são todas as ferramentas que permitem ao sistema interagir com o ambiente gerando dados de forma rápida como câmaras, microfones, sensores de movimento, de temperatura ou de pressão (Fernandes, 2020). Os algoritmos definem-se pelas sequências de instruções introduzidas pelo homem no sentido de preparar o computador para unir pontos de acontecimentos que de forma isolada parecem inofensivos, mas em conjunto criam um padrão ameaçador. Desta forma, os algoritmos funcionam como um radar preditivo capaz de antecipar e evitar manobras do adversário procurando uma resposta (Moleirinho, 2021).

Os *metadados*, ou *big data*, são definidos como os dados colhidos sobre outros dados, como a videovigilância em que a visualização de um veículo irá gerar múltiplos dados classificando-os pela sua cor, direção de movimento, forma, velocidade, entre outros, criando assim novos dados (Security Magazine, 2021).

A capacidade de um computador aprender autonomamente algo para o qual não se encontra programado é definida por *machine learning* (Samuel, 1959), onde um algoritmo funciona com um conjunto de dados de treino que ensina a máquina a potenciar os seus atributos para conseguir identificar as suas características no futuro (Bini, 2018). Jakhar & Kaur (2020) definem o *machine learning* como a criação de algoritmos capazes de aprender autonomamente, fazer previsões de dados e tomarem decisões baseadas em modelos pré delineados pelo homem. Como exemplo desta aplicabilidade existe, no âmbito da agricultura, a máquina industrial Trapic, que através de ferramentas de visão consegue captar o sistema de características dos morangos permitindo encontrá-los a uma

determinada distância, avaliar o seu estado de maturação através da cor e, recolhê-los, caso estejam no ponto de maturação ideal (Lee, 2018).

Da definição *machine learning* surge o *deep learning* que se distingue pela possibilidade que os dados têm em se apresentarem em vários formatos graça às camadas de redes neuronais (Lecun et al, 2015). Existe uma sequência de camadas de processamento de dados onde cada uma gera um *output* que servirá de *input* da camada seguinte fazendo com que o algoritmo vá aprendendo e aperfeiçoando a sua eficácia, permitindo à máquina aprender por si sem haver necessidade de introduzir parâmetros. Como exemplo temos a capacidade que a máquina tem em identificar a mesma pessoa em duas fotos diferentes (Jakhar & Kaur, 2020). Segundo Lee (2018) quanto maior exposição os algoritmos tiverem a dados, maior será a sua capacidade para processar características e relações entre os mesmos. Como exemplo de aplicabilidade do *deep learning* é a empresa RXThinking que utiliza algoritmos para detetar doenças. O programador limitou-se a introduzir alguns dados como sintomas da doença e a máquina, após análise de casos semelhantes que possua na sua base de dados, vai preparar o diagnóstico mais provável, bem como outras possíveis causas de sintomas (Lee, 2018).

Outro conceito importante para o presente estudo é o de vídeo analítico, também designado como análise inteligente de vídeo, que se baseia numa tecnologia com a capacidade de proceder à desconstrução de imagens de vídeo, com o objetivo de detetar e identificar ações e objetos automática e autonomamente (Segurança Eletrónica, 2022). Mais uma das capacidades de IA agregada à Visão Computacional, onde câmaras podem ser equiparadas aos olhos de um ser humano e o sistema de vídeo analítico pode ser equiparado ao cérebro que vai analisar, compreender e processar o que visualiza, sendo as possibilidades de aplicação de tal forma vastas (e em constante mutação), desde a tecnologia termográfica, a simples deteção de elementos específicos, o cruzamento de linha virtual, a *ROI – Region of Interest*, sentido de movimento, reconhecimento de comportamentos, contagens de elementos até o rastreamento desses elementos na imagem e o reconhecimento facial (Security Magazine, 2022; Segurança Eletrónica, 2022).

A tecnologia termográfica tem a capacidade de deteção de fumo e fogo, inundações em cenários onde a iluminação é escassa, temperatura de pessoas e objetos e processando alertas para o utilizador (Security Magazine, 2022).

A deteção de elementos específicos consiste na introdução de informação sobre a existência de objetos (pessoas, animais, bicicletas, veículos, entre outros) que irá despoletar a criação de dados e fazendo com que os algoritmos, através da tecnologia

baseada em *deep learning*, reconheçam os objetos apesar das suas formas e cores diferenciadas (Segurança Eletrónica, 2022).

A linha virtual é uma linha imaginária que se divide por setores o que está a ser vigiada no sentido de capacitar o sistema de interpretações diferentes e objetivos diferentes para a mesma câmara (Segurança Eletrónica, 2022).

A *ROI – Region of Interest* segue a mesma aplicabilidade da linha virtual mas com o objetivo de controlar uma área, criando um alto nível de processamento para essa zona com alertas específicos como a monitorização por videovigilância de uma garagem coletiva onde só é permitida a passagem de veículos e proibida a de pessoas. Ao criar um ROI na entrada da garagem, e apesar da movimentação de vários veículos, o programa irá identificar a passagem de pessoas criando um alerta no sistema de vídeo analítico (Segurança Eletrónica, 2022).

O sentido de movimento, associada à função da linha virtual, habilita o sistema de uma análise do sentido do movimento das pessoas podendo servir de alerta para locais com elevada confluência de pessoas (metro, eventos de massa, entre outros) onde se verifique um incidente havendo alterações drásticas de movimentos diferentes das que estavam a ser adotadas anteriormente. Em situações de gestão de tráfego de pessoas e trânsito o sistema pode estar acoplado aos semáforos de controlo rodoviário e fazer uma gestão integrada de fluxo entre viaturas e peões (cruzamentos, passadeiras, entre outros) (Segurança Eletrónica, 2022).

O reconhecimento de comportamentos é outra capacidade do vídeo analítico que subsiste na setorização de dados que geram comportamentos que são pré identificados aos algoritmos. O sistema aprende a identificar diferentes movimentos que geram o mesmo comportamento e é bastante utilizado em centros comerciais e lojas de venda a público com a deteção de furtos, roubos, ofensas à integridade física e acidentes rodoviários. (Segurança Eletrónica, 2022).

A contagem de elementos que, tal como o nome indica, é outra tecnologia muito utilizada pelo sector empresarial e autarquias para o controlo e análise do fluxo de pessoas e veículos, tempos de duração e permanência, sendo uma ferramenta bastante útil no auxílio à compreensão dos movimentos diários da sociedade (Segurança Eletrónica, 2022).

O reconhecimento facial tradicional baseia-se na existência de uma base de dados onde um grupo de pessoas estão “registados” e o sistema analítico vai fazer a análise biométrica das características individuais presentes nos traços de rosto de cada um (distância entre olhos, tamanho do queixo, a linha da mandíbula, entre outros), e através da

leitura e comparação dos dados é possível identificar uma pessoa. Este é o método mais usual em países onde é permitido a utilização de dados biométricos, porém a tecnologia já permite identificar pessoas através de características físicas como altura, indumentária, forma de andar, idade, género, entre outras características. Também já é possível identificar a partir de uma fotografia onde o sistema vai criar dados sobre os traços individuais e procurar no sistema CCTV se aquela pessoa se encontra em local vigiado ou se já lá esteve no passado (Intelbras, 2020).

Hipóteses teóricas

A UE tem-se debruçado sobre as implicações da evolução da IA para a economia mundial, os riscos associados que podem por em causa Direitos, Liberdades e Garantias (DLG) e a proteção de dados pessoais. O Livro Branco sobre a inteligência artificial (Comissão Europeia, 2020b) define as opções políticas sobre a forma de alcançar o duplo objetivo: promover a adoção de IA e identificar os riscos associados a determinadas utilizações. Assim e com o objetivo de uniformizar procedimentos para o controlo dos riscos foi elaborado posteriormente um Regulamento do Parlamento Europeu para a IA (Comissão Europeia, 2021) onde se pretende um elevado nível de proteção de direitos fundamentais dos cidadãos da UE quando utilizam IA, promovendo, em simultâneo, o desenvolvimento da tecnologia. Nesse regulamento estão previstas orientações que os países membros terão que adotar.

Em Portugal existem várias normas que regulam a videovigilância de particulares e entidades públicas onde as competências para a autorização, implementação e fiscalização podem recair em várias entidades do Estado. Considerando o impacto desta tecnologia, a sua constante evolução, as orientações emanadas pela UE, as dúvidas relativas à preservação de DLG, consideramos que muito está por fazer na aplicação da tecnologia em prol da segurança e na fiscalização da sua aplicação no setor público e privado. Sob esta base, definimos as seguintes questões de investigação: Q1. A legislação portuguesa é clara e está adequada à salvaguarda dos direitos dos cidadãos e valores éticos no que respeita à aplicação de sistemas de IA em videovigilância? Q2. Através de alterações legislativas, poderá a PSP afirmar-se nesta temática tornando-se autoridade fiscalizadora para os sistemas de IA em videovigilância? Tendo por base a revisão da literatura efetuada e a experiência na monitorização de sistemas de CCTV e sua fiscalização, formulamos as seguintes hipóteses: H1. A legislação portuguesa é adequada, independentemente de estar ou não a ser corretamente aplicada. H2. A legislação portuguesa não é adequada, por não responder de forma satisfatória às necessidades de prevenção e controlo.

O método adotado resultou da natureza teórica do presente estudo, pelo que recorremos à revisão da literatura e análise documental sobre este tema.

Perspetivas e Diretrizes

Normativos europeus

Em comunicado elaborado em 2018, a UE iniciou o caminho da concordância dos países membros para a adoção de políticas comuns de reforço da capacidade industrial e tecnológica, a adoção de IA e a criação de um quadro jurídico e ético adequado (Comissão Europeia, 2018) que vise o cumprimento dos Direitos Fundamentais da UE (União Europeia, 2012) e a garantia do devido tratamento dos dados pessoais e a livre circulação dos mesmos previstos no Regime Geral da Proteção de Dados (Comissão Europeia, 2016).

Em 2020 a UE elaborou um plano estratégico, 2020-2025, para a união da segurança dos Estados membros em matéria de ameaças em constante evolução, proteção contra o terrorismo e criminalidade organizada e políticas de um ecossistema de segurança europeu solido (Comissão Europeia, 2020a). Este documento refere que os benefícios associados à globalização, livre circulação e transformação tecnológica e digital comportam riscos facilitadores do terrorismo e da criminalidade organizada potenciadores de ameaças à segurança da UE. Mais acrescenta que a segurança e o respeito pelos DLG podem-se complementar, devendo constituir um desidrato de uma política assente em valores comuns europeus (Comissão Europeia, 2020a).

A CE emitiu ainda o Livro Branco da IA (Comissão Europeia, 2020b) que veio criar as diretrizes que sustentam o Regulamento da IA criado em 2021 (Comissão Europeia, 2021) e que se encontra neste momento a ser transposto para os ordenamentos jurídicos dos países membros. O Regulamento faz uma abordagem à IA classificando-a em níveis definidos de acordo com a complexidade e riscos associados – práticas de IA proibidas, sistemas de IA de risco elevado e outros sistemas de IA de interação com pessoas singulares. Esta regulamentação é aplicada aos fornecedores de tecnologia dos Estados membros e de países terceiros que queiram colocar sistemas de IA no mercado da UE (Comissão Europeia, 2021).

A prática de IA proibidos, ou nocivos, encontra-se prevista no II Título do regulamento e comporta, essencialmente, todos os sistemas intrusivos que empreguem técnicas subliminares para controlo da consciência humana; distorção de comportamento de pessoas; a recolha e tratamento de dados de pessoas singulares ou grupos com vista à utilização noutros contextos com fins prejudiciais e desfavoráveis, injustificados e desproporcionais aos dados colhidos inicialmente pelos algoritmos; a utilização de

sistemas de identificação biométrica à distância, em tempo real, para controlo da ordem pública. Relativamente a esta última utilização nociva, a UE refere que podem haver exceções abrindo a possibilidade de utilizar o controlo biométrico, em tempo real, caso se afigure necessário para a manutenção da ordem pública para casos de investigação específica de potenciais vítimas de crimes relacionadas com crianças desaparecidas, prevenção de uma ameaça específica contra a vida de pessoas ou ataque terrorista ou deteção, localização, de suspeito de infração penal com pena privativa da liberdade não inferior a 3 anos previstos no artigo 2º, n.º 2 da Decisão-quadro 2002/584/JAI (Comissão Europeia, 2021). Neste normativo encontramos identificados os tipos de crimes mais usuais que servem de argumento para a implementação da videovigilância em Portugal tais como homicídio, ofensas graves à integridade física, roubo, tráfico de seres humanos, tráfico de armas, tráfico de estupefacientes, rapto, sequestro, tomada de reféns e violação (Decisão-quadro, 2002).

Os sistemas de IA de risco elevado, apresentados no III Título do regulamento, são todos os sistemas que afetam negativamente a segurança dos cidadãos, havendo uma necessidade de cumprir determinados requisitos de qualidade, apresentação de documentação técnica, transparência, controlo e supervisão humana na aplicação do sistema de IA. Aqui se enquadram várias valências da IA para o apoio à investigação criminal das autoridades policiais tais como avaliações de riscos de reincidências na atividade criminosa, sistemas de deteção de estados emocionais de pessoas funcionando como polígrafos, sistemas que detetam falsificações e sistemas de apoio à investigação (Comissão Europeia, 2021).

Os outros sistemas de IA de risco limitado são os mais presentes na UE, sendo os requisitos mais específicos principalmente na transparência o que obriga a que todos os seus utilizadores tenham conhecimento das capacidades de IA. A utilização de IA em ambiente de teste também está prevista no regulamento, assim como a sua supervisão e a obrigatoriedade em apagar os dados pessoais tratados logo após o *términus* do teste (Comissão Europeia, 2021).

No VI Título do regulamento está prevista a criação de um Comité Europeu para a IA que presta aconselhamento e assistência à CE. O Comité é composto por um novo órgão – autoridades nacionais de controlo de cada Estado-Membro, e pela Autoridade Europeia para a Proteção de Dados. As autoridades nacionais de controlo são responsáveis pela execução e aplicação do presente regulamento e pela coordenação das atividades confiadas pelo Estado-Membro e possuem funções de autoridade notificadora e autoridade

fiscalizadora do mercado. Podem ser criadas mais do que uma autoridade nacional de controlo por razões organizacionais e administrativas do seu Estado-Membro. Está prevista a dotação de recursos financeiros e humanos adequados para o exercício destas funções e os recursos humanos devem ter competências e conhecimentos especializados que incluam uma compreensão profunda das tecnologias de IA, dos dados, dos direitos fundamentais, dos riscos para a saúde e segurança (Comissão Europeia, 2021).

No artigo 63º, n.º 5, do regulamento, a CE permite que o Estado-Membro decida de entre duas autoridades aquela que ficará responsável (autoridade nacional de controlo) pelos sistemas de IA utilizados para a identificação biométrica à distância e em tempo real para efeitos de manutenção de ordem pública e os sistemas já referidos como risco elevado de várias valências da IA para o apoio à investigação criminal das autoridades policiais. Desta forma, existe a possibilidade de decisão entre a autoridade de controlo no domínio da proteção de dados – Comissão Nacional de Proteção de Dados (CNPD), e as autoridades nacionais competentes para a manutenção da ordem pública, imigração ou asilo que colocam em serviço ou utilizam esses sistemas.

Um fornecedor de um produto de IA de risco elevado tem de garantir que o sistema cumpre as normas estipuladas pela UE, criar um documento técnico do sistema e submete-lo ao procedimento da avaliação de conformidade antes de o colocar no mercado conforme refere o III capítulo do regulamento. A autoridade de controlo notifica o organismo de avaliação de conformidade (estes tem de cumprir os preceituados no artigo 33º) que por sua vez avalia, aprova e, após a remessa do processo para o Comité Europeu e Estados-membros, se ninguém se opuser à implementação do novo sistema, o fornecedor recebe a certificação e conformidade CE podendo operar em qualquer país da UE. Este regulamento é aplicável a partir de vinte e quatro meses após a sua entrada em vigor (Comissão Europeia, 2021).

A Videovigilância de locais públicos e de utilização comum em Portugal

A videovigilância operada pelas FS em locais públicos de utilização comum, foi inicialmente regulada pela Lei n.º 1/2005, de 10 de janeiro com sucessivas alterações. Existiram contudo algumas utilizações de sistemas CCTV anteriores ao ano de 2005 tais como no evento *Expo 98* sem enquadramento legal à data (Carvalho, 2020). Como essa ferramenta demonstrou ser uma mais-valia para o sucesso do evento no que à prevenção criminal diz respeito, não foi alvo de qualquer contestação (Chambel, 2000). Antes da criação do diploma legal para a utilização de sistemas de CCTV na via pública, surgiu a necessidade de regular a utilização deste sistema no domínio privado e nomeadamente ao

nível do setor da segurança privada (Decreto-lei n.º 35/2004, de 21 de Fevereiro, revogado). Posteriormente alguns prestadores de serviços privados passaram a ter a obrigação de instalar sistemas de CCTV como os postos de abastecimento, farmácias e instituições de crédito, com a entrada em vigor da Lei n.º 34/2013, de 16 de maio.

Nos primeiros anos de aplicação da Lei n.º 1/2005, de 10 de janeiro, não se viu um processo evolutivo tendo sido marcado por controvérsias e discórdias entre as entidades responsáveis: autarquias, Ministério da Administração Interna (MAI), FS e CNPD. As autarquias ou FS formalizavam o pedido devidamente fundamentado e sustentado na necessidade de prevenção criminal em locais onde existisse razoável risco de ocorrência, posteriormente seguia para o MAI que analisava e aprovava seguindo por fim à CNPD que lhes competia dar um parecer, sendo este, à época, vinculativo. As argumentações dos pedidos eram escrutinadas pela CNPD e tornou-se difícil justificar a proporcionalidade e adequação do uso de sistemas CCTV uma vez que a função desta entidade é a garantia do equilíbrio entre direitos fundamentais e a segurança (Frois, 2015). Esta lei sofreu quatro alterações sendo a atual a Lei n.º 95/2021, de 29 de dezembro. Uma das maiores alterações foi o desvinculo da obrigação de ter um parecer positivo da CNPD para a validação de um sistema de CCTV. O parecer continua a ser necessário, mas não é vinculativo competindo ao membro do governo que exerce a direção sobre a força ou serviço de segurança a autorização de instalação. Dos vários fins a que se destinam estes sistemas de CCTV, previstos no artigo 3º, surge a prevenção de atos terroristas como um dos argumentos para a instalação que não estava anteriormente previsto. A duração máxima da autorização passa de dois para três anos, suscetível de renovação por período igual ou inferior, caso os pressupostos iniciais que levaram à autorização se mantenham (artigo 7º, n.º 2). Surge a autorização de sistemas de gestão analítica dos dados captados desde que, no pedido inicial, surja a descrição técnica do sistema de IA (artigo 6º, n.º 1). É permitida a recolha e tratamento de dados, contudo não é permitida a captação e tratamento de dados biométricos conforme o artigo 16º. A CNPD mantém o poder de fiscalização sobre os dados recolhidos e seu tratamento (artigo 24º) e as características técnicas dos sistemas CCTV, estão previstas na Portaria n.º 372/2012.

Desta forma, no contexto atual, as FS em parceria com as autarquias apresentam um projeto de instalação de sistema de CCTV, proposto ao MAI que após o parecer não vinculativo da CNPD, decide positiva ou negativamente. Caso seja autorizado, a instalação e manutenção fica ao encargo da autarquia, e a operacionalização a cargo da FS territorialmente competente. A central de receção e monitorização fica instalada no centro

de comando e controlo operacional da Divisão/Comando. As câmaras encontram-se ligadas por uma rede de fibra ótica e a comunicação entre elas é encriptada. As câmaras permitem movimento *pan & tilt* (rotação horizontal e vertical), zoom, policromáticos de visão noturna em modo patrulha, analítica de vídeo consoante as necessidades de cada local (Pereira, 2017).

No que respeita aos locais de domínio privado, mas acessíveis ao público, existem alguns normativos orientadores da videovigilância. Considerando as pessoas particulares e a segurança do domínio da propriedade privada (residências), a mesma é legítima não necessitando de qualquer autorização, tendo apenas de cumprir com o estipulado no artigo 19º, da Lei n.º 58/2019, de 8 de agosto (limites para a sua instalação – proteção de dados). Para as restantes situações os sistemas de videovigilância de controlo privado são considerados meios de segurança privados e estão previstos no Regime de Exercício da Segurança Privada (LSP) (Lei n.º 46/2019, de 8 de julho). Nesta LSP existem medidas de segurança obrigatórios para estabelecimentos tais como instituições bancárias, ourivesarias, farmácias e centros comerciais, onde se destaca o sistema CCTV. Tal vem previsto na LSP e no VIII Capitulo da Portaria n.º 273/2013. Para as empresas que, não sendo obrigadas, queiram introduzir um sistema de CCTV devem adquiri-lo no mercado nacional em empresas com alvarás conforme previsto no artigo 14º e cumprir os requisitos constantes na LSP. É autorizada a instalação de sistemas de CCTV para proteger pessoas e bens e prevenir a prática de crimes.

Compete à Direção Nacional da PSP (DNPSP) a instrução dos processos de autorização para o exercício de atividades de segurança privada nos quais se engloba a instalação de sistemas de CCTV e as centrais de receção e monitorização da videovigilância (artigo 42º da LSP). A fiscalização das atividades reguladas na LSP é assegurada pela DNPSP em articulação com a Autoridade para as Condições do Trabalho a Autoridade Tributária e Aduaneira, sempre que se afigure necessário (artigo 55º da LSP). Compete também à DNPSP a tramitação de toda a ação de controlo, licenciamento e fiscalização para sistemas de informação digitais. A DNPSP faz parte do Conselho de Segurança Privado, como outros organismos do Estado, contudo tem um papel preponderante prestando o apoio técnico e administrativo necessários ao funcionamento deste órgão (artigo 39º da LSP) uma vez que é a autoridade administrativa que retém o domínio do licenciamento e fiscalização do exercício da atividade de segurança privada.

Discussão

A UE está empenhada em construir um mercado económico mais competitivo e tecnológico com o desenvolvimento de tecnologias de IA. Como já referido, o investimento está a ser realizado em vários setores da sociedade, contudo ainda não verificamos nenhum projeto nacional com vista a uma transformação da tecnologia ligada à segurança interna. Em contrapartida, o setor privado tem evoluído e as empresas têm investido na segurança dos seus produtos e dos seus clientes, desenvolvendo ou adquirindo sistemas de IA nas várias vertentes (gestão de recursos humanos, robótica, segurança, entre outros). Se o setor privado investe em segurança é porque o mercado está recetivo à aceitação da observação coletiva em prol da segurança de pessoas e bens. Segundo Pereira (2017),

> Os sistemas de videovigilância a implementar em espaços públicos de utilização comum constituem uma valiosa ferramenta e instrumento complementar da actividade policial, preventiva e reativa. Além de uma capacidade preventora, estes sistemas permitem também agilizar e maximizar a resposta policial a cada situação em concreto, facilitando, de igual modo, as diligências no domínio da investigação criminal (p.3).

Partilhamos do mesmo entendimento de Pereira (2017) quando refere que Portugal propende a seguir a tendência europeia no sentido de fornecer à FS uma maior intervenção no domínio dos sistemas de CCTV.

Em Portugal existem 900 câmaras de filmar em 14 cidades. Apesar de ser aparentemente pouco, ressalva-se que em 2013 existiam 38 câmaras (Ferreira, 2022) pelo que se verifica um aumento substancial e um esforço por parte dos municípios envolvidos. A existência de um volume elevado de câmaras de videovigilância para um operador monitorizar em tempo real e, num turno de serviço, torna o processo ineficaz na medida em que é humanamente impossível o ser humano manter elevados níveis de atenção e não se conseguir supervisionar todas as câmaras simultaneamente.

Neste contexto, a utilização de recursos tecnológicos de CCTV por parte das FS, tem assumido preponderância e mais-valia na vigilância de espaços públicos, aportando, questões relacionadas com a salvaguarda de DLG, sobretudo a proteção de dados pessoais (Albuquerque, 2022). É exigido, diariamente às FS, uma resposta cabal de visibilidade e proximidade com as comunidades, contudo estas vêem-se limitadas pelas reduções de

recursos humanos e racionalização de custos (Dias, 2012). A utilização de sistemas de CCTV com IA incorporados potencia a eficiência dos recursos a aplicar e a eficácia dos resultados alcançados, quer na prevenção como na investigação criminal (Albuquerque, 2022).

Após a análise das potencialidades das ferramentas de IA para a videovigilância, consideramos que se deve retirar partido do máximo de potencialidade dos sistemas de IA, atribuindo ao operador a competência para analisar os alertas emitidos pelo sistema e direcionar os meios, caso se confirme os alertas detetados pelos algoritmos instalados em função das várias valências aqui já anunciadas na analítica de vídeo.

Dentro desta gestão analítica de vídeo, uma ferramenta que põe em causa a proteção de dados pessoais é o controlo biométrico que, na legislação portuguesa não é permitido em sistemas de CCTV. Desta forma, o Regulamento Europeu para a IA permite, a utilização de dados biométricos pelas FS, sendo esta a única prática nociva de IA a ser aplicada em situações que estejam em causa a resolução de uma situação criminal, havendo um conflito entre a legislação portuguesa e o regulamento europeu. No quadro legislativo português, a Lei n.º 58/2019, de 8 de agosto (Lei de Proteção de Dados Pessoais) e a Lei n.º 59/2019, de 8 de agosto (regras relativas ao tratamento de dados pessoais para efeitos de investigação ou repressão de sanções penais), ambas referentes à proteção e tratamento de dados pessoais, nada referem sobre critérios específicos para a aplicação de IA, produção de dados, metadados e algoritmos. Estas leis são anteriores ao Livro Branco sobre a IA e ao Regulamento Europeu da IA. A Lei n.º 95/2021, de 29 de dezembro (utilização e o acesso das FS a sistemas de CCTV), apesar de ter sido publicada posteriormente ao Regulamento Europeu da IA, admite a possibilidade de tratamento de dados através de um sistema de gestão analítico de dados, de acordo com os fins a que se destinam os sistemas, contudo nada refere sobre critérios específicos para a aplicação de IA, produção de dados, metadados e algoritmos (Albuquerque, 2022). Em suma, podemos afirmar que o quadro legislativo português atualmente em vigor não se encontra enquadrado com as políticas europeias nomeadamente ao que se refere o Regulamento Europeu para a IA. Independentemente das alterações legislativas a ser produzidas há a necessidade da criação da autoridade de controlo, autoridade notificadora e autoridade de fiscalização (ou várias conforme anteriormente referido) para a IA. Criar as orientações para a certificação de sistemas de IA, controlo e fiscalização dos mesmos conforme preceituado no regulamento. Desta forma consideramos que, em resposta à primeira questão levantada na elaboração deste estudo, a legislação portuguesa não é adequada, por

não responder de forma satisfatória às necessidades de prevenção e controlo, pelo que deve ser promovida a discussão com vista à sua alteração e criação de mecanismos de controlo e fiscalização.

Na sintetização dos principais artigos do Regulamento Europeu para IA verificou-se que deverá ser criada uma autoridade nacional de controlo que fará parte do Comité Europeu para a IA. Esta deverá ser dotada de recursos financeiros e humanos adequados para o exercício das suas funções de controlo e fiscalização. Os seus funcionários devem estar dotados de competências e conhecimentos especializados que incluam uma compreensão profunda das tecnologias de IA, dos dados e da computação de dados (artigo 59º do Regulamento Europeu para IA). Atendendo à complexidade técnica desta autoridade somos do entender que deverá ser criada uma Autoridade Nacional de Controlo de raiz. Contudo, podem ser criadas outras autoridades nacionais competentes por razões organizacionais e administrativas, mencionando o artigo 63º vários exemplos de autoridades nacionais competentes para a fiscalização, nas quais se destaca o MAI no campo da utilização de sistemas de IA concebidos para serem utilizados para a identificação biométrica à distância. Aqui a PSP, enquanto autoridade administrativa para atividade de segurança privada e, sendo nesta que se enquadram as obrigações de existência de sistemas de CCTV ou imposições de regras por parte de espaços privados de acesso ao público, consideramos que poderá ter um papel ativo na fiscalização, assumindo funções de autoridade nacional de fiscalização de IA, por delegação de competências, sobre esta matéria. Assim, vemos respondida a segunda questão de investigação criada na formulação do problema.

Conclusões

A globalização e a evolução tecnológica criam desafios e ameaças às sociedades atuais, obrigando-as a conjugar esforços, para promover a segurança, numa conjugação de políticas e valores comuns na comunidade europeia e na salvaguarda de DLG. A transposição do Regulamento Europeu para a IA irá requerer um esforço suplementar da Assembleia da República na organização do regulamento interno pois será um marco na transformação tecnológica nos vários setores da sociedade. Como concluímos, a legislação atualmente em vigor no que se refere à proteção de dados e à videovigilância, terá de sofrer alterações com vista à implementação destes sistemas tecnológicos. A PSP poderá e, deverá, ter um papel preponderante na fiscalização de sistemas de CCTV com IA, por todo o conhecimento e experiência nesta matéria.

A limitação de 3 anos que a atual legislação impõe aos municípios que queiram instalar um sistema de CCTV, por serem ferramentas que requerem um investimento monetário avultado, pode ser um fator limitador e constrangedor desse investimento, pelo que consideramos que este prazo deva ser alargado. Entendemos que seria uma mais-valia de adoção de um sistema integrado de videovigilância urbano, onde os processos se continuariam a iniciar num protocolo de colaboração entre autarquia e comando territorial mas sobre a supervisão e orientação de um serviço central da DNPSP que, no nosso entender, devia estar na dependência do Departamento de Segurança Privado, por toda a sua competência e conhecimento nas medidas de segurança privada. A ser exequível, a criação de uma Divisão de controlo e monitorização de sistemas de CCTV iria deter o domínio de todos os processos de instalação, comunicação com o MAI e supervisão de todos os sistemas de CCTV públicos urbanos e fiscalização dos sistemas privados de CCTV.

Por fim, reconhecemos várias limitações a este estudo, pela pouca bibliografia de IA direcionada para a segurança e as que existem, na sua maioria, advêm de países onde DLG não são atendíveis em comparação com a segurança interna. Por considerarmos este tema de elevada importância para a segurança interna, entendemos como importante o desenvolvimento de estudos e debates relativos ao uso de IA entre peritos e FS.

Referências

Albuquerque, S. I. dos S. Q. (2022). *O impacto da tecnologia no policiamento.* [Trabalho de investigação individual do CEMC não publicado]. Instituto Universitário Militar. https://comum.rcaap.pt/handle/10400.26/41640

Bini, S. A. (2018). Artificial intelligence, machine learning, deep leraning, and cognitive computing: What do these terms mean and how will theyimpact health care? *The Journal of Arthroplasty*, 33 (8), 2358-2361 https://www.arthroplastyjournal.org/article/S0883-5403(18)30215-8/fulltext

Cabral, J. A. H. S. (2011). Do direito à segurança do Direito. *Proceedings of the Fourth International Conference on The Legal Reforms of Macau in Global Context.* Faculdade de Direito da Universidade de Macau. https://www.stj.pt/wp-content/uploads/2018/01/macaufaculdadedireito.pdf

Carvalho, I. O. (2020). *Sistemas de videovigilância na freguesia de Águas Livres: Efeitos na criminalidade.* [Dissertação de Mestrado Integrado em Ciências Policiais não publicado]. Instituto Superior de Ciências Policiais e Segurança Interna. https://comum.rcaap.pt/bitstream/10400.26/32978/1/155861_Carvalho_Sistema-de-videovigil%C3%A2ncia-na-freguesia-de-%C3%81guas-Livres-Efeitos-na-criminalidade_VERSAOFINAL.pdf

Chambel, É. M. (2000). *Videovigilância em locais de domínio público de utilização comum.* [trabalho de final de curso em Ciências Policiais não publicado]. Instituto Superior de Ciências Policiais e Segurança Interna.

Comissão Europeia. (2016). Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de Abril. *Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados.* Jornal Oficial da União Europeia, L119/89 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680&from=HU

Comissão Europeia. (2018). *Inteligência artificial para a Europa*. COM (2018) 237 final https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52018DC0237

Comissão Europeia. (2020a). *Estratégia da EU para a União da Segurança*. COM (2020) 65 final https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52020DC0605

Comissão Europeia. (2020b). *Livro Branco sobre a inteligência artificial – Uma abordagem europeia virada para a excelência e a confiança*. COM (2020) 65 final https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52020DC0065

Comissão Europeia. (2021). *Regulamento do parlamento europeu e do conselho que estabelece regras harmonizadas em matéria de inteligência artificial (regulamento de inteligência artificial) e altera determinados atos legislativos da união.* COM (2021) 206 final https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52021PC0206

Dean, J. (2012). How many to identify a cat? 16,000. *The New York Times*. https://www.nytimes.com/2012/06/26/technology/in-a-big-network-of-computers-evidence-of-machine-learning.html

Decisão-quadro 2002/584/JAI. *Relativa ao mandando de detenção europeu e aos processos de entrega entre Estados-Membros.* Jornal Oficial da União Europeia, L190, 1-20 https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32002F0584

Dias, M. D. A. (2012). *Um olhar conjuntural em torno da (s) política (s) (d)e segurança.* Fonte da Palavra

Fernandes, L. F. (2020). Inteligência artificial. Desafios e oportunidades para a Polícia. *Revista Polícia Portuguesa*, 5(2), 30-35 https://www.researchgate.net/publication/349042943_Inteligencia_Artificial_Desafios_e_Oportunidades_para_a_Policia

Ferreira, M. (2005). *Princípios fundamentais porque se deve pautar a acção policial num Estado de direito democrático.* Almedina

Ferreira, R. da R., (2022). Há 900 câmaras autorizadas para vigiar ruas. Em breve deverão ser mais de 1200. *Exame Informática.* https://visao.sapo.pt/exameinformatica/serie-vigiados/2022-09-07-camaras-videovigilancia-ruas-portugal/

Frois, C. (2011). *Vigilância e poder*. Mundos sociais https://www.mundossociais.com/temps/livros/11_30_11_15_vigilanciafftindiceprfint.pdf

Frois, C. (2015). Segurança em crise: Dez anos de videovigilância na via pública em Portugal. In Fonseca, C. & Machado, H. (Organizadoras) *Ciência, identificação e tecnologias de governo*. (p. 222-234) Centro de Estudos Internacionais sobre Governo. Editora UFRGS https://www.lume.ufrgs.br/bitstream/handle/10183/213251/001114121.pdf?sequence=1

Fundação para a Ciência e Tecnologia. (2021). *AI Portugal 2030. Portuguese national initiative on digital skills.* Incode2030 https://www.portugal.gov.pt/download-ficheiros/ficheiro.aspx?v=%3D%3DBAAAAB%2BLCAAAAAAABACzMDQxAQC3h%2ByrBAAAAA%3D%3

Giddens, A. (2005). *Sociologia.* (4ª ed). Tradução Sandra Regina Netz. Artmed

Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*. 61(4), 5-14. https://www.researchgate.net/publication/334539401_A_Brief_History_of_Artificial_Intelligence_On_the_Past_Present_and_Future_of_Artificial_Intelligence

Hempel, L., & Topfer, E. (2002). Inception report. *Centre for Tecnology and Society.* Technical University Berlin. http://www.urbaneye.net/results/ue_wp1.pdf

Intelbras, (2020). *Câmara com reconhecimento facial: conheça essa tecnologia.* Consultado a 22 de 01 de 2023. https://blog.intelbras.com.br/camera-com-reconhecimento-facial-conheca-essa-tecnologia/

Jakhar, D., & Kaur, I. (2020) Artificial intelligence, machine learning and deep learning: definitions and diferences. *Clinical and experimental dermatology*, 45(1), 131-132 https://academic.oup.com/ced/article/45/1/131/6597747?login=false

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature,* 521(7553), 436-444 https://www.nature.com/articles/nature14539

Lee, K. F. (2018). *As superpotências da inteligência artificial: a China, Silicon Valley e a Nova Ordem Mundial.* Tradução Maria Eduarda Cardoso. Relógio D'Àgua

Lei n.º 1/1976, de 10 de Abril. Aprova a Constituição da República Portuguesa. Diário da República n.º 86/1976: I Série de 10 de abril. https://dre.pt/dre/detalhe/decreto-aprovacao-constituicao/1976-502635

Lei n.º 46/2019, de 8 de julho. Altera o regime do exercício da atividade de segurança privada e da autoproteção. Diário da República n.º 128/2019: I Série de 8 de julho. https://dre.pt/dre/detalhe/lei/34-2013-122996202

Lei n.º 53/2007, de 31 de agosto. Aprova a orgânica da PSP. Diário da República n.º 168/2007: I Série de 31 de agosto. https://dre.pt/dre/legislacao-consolidada/lei/2007-174279072-174336179

Lei n.º 53/2008, de 29 de agosto. Aprova a Lei de Segurança Interna. Diário da República n.º 167/2008: I Serie de 29 de agosto. https://dre.pt/dre/legislacao-consolidada/lei/2008-34501675

Lei n.º 58/2019, de 8 de agosto. *Assegura a execução, a ordem jurídica nacional, do regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção de pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados*. Diário da República n.º 151/2019: I Serie de 8 de agosto. https://dre.pt/dre/detalhe/lei/58-2019-123815982

Lei n.º 59/2019, de 8 de agosto. *Aprova as regras relativa ao tratamento de dados pessoais para efeitos de prevenção, deteção, investigação ou repressão de infrações penais ou de execução de sanções penais.* Diário da República n.º 151/2019: I Série de 8 de agosto. https://dre.pt/dre/detalhe/lei/59-2019-123815983

Lei n.º 95/2021, de 29 de dezembro. *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 a captação, gravação e tratamento de imagem e som.* Diário da República n.º 251/2021: I Série de 29 de dezembro. https://dre.pt/dre/detalhe/lei/95-2021-176714548

Moleirinho, P. (2018). A importância dos modelos preditivos na área da segurança. Entre riscos e equilíbrios instáveis. *Modelos preditivos e segurança pública.* Fronteiras do Caos Editoras Lda. 99-130 http://sim4security.novaims.unl.pt/wp-content/uploads/2016/11/Modelos-Preditivos-e-Seguranca-Publica.pdf

Moleirinho, P. M. S. E. (2021). *Aplicação da inteligência artificial ao serviço da função policial.* [Trabalho de investigação individual do Curso de Promoção a Oficial General não publicado]. Instituto Universitário Militar. http://hdl.handle.net/10400.26/38136

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

Pereira, L. A. S. P. (2017). *Políticas de segurança e a videovigilância urbana – O caso da Amadora.* [Trabalho de investigação final do IV Curso de Direção e Estratégia Policial não publicado]. Instituto Superior de Ciências Policiais e Segurança Interna. http://hdl.handle.net/10400.26/35180

Portaria n.º 272/2013, de 20 de agosto. *Define os requisitos e o procedimento de registos, na Direção Nacional da Polícia de Segurança Pública (PSP), das entidades que procedam ao estudo e conceção, instalação, manutenção ou assistência técnica de material e equipamento de segurança ou de centrais de alarme.* Diário da República n.º 159/2013: I Série de 20 de agosto. https://dre.pt/dre/detalhe/portaria/272-2013-499241

Portaria n.º 273/2013, de 20 de agosto. *Regula as condições específicas da prestação dos serviços de segurança privada, o modelo de cartão profissional e os procedimentos para a sua emissão e os requisitos técnicos dos equipamentos, funcionamento e modelo de comunicação de alarmes.* Diário da República n.º 159/2013: I Série de 20 de agosto. https://dre.pt/dre/detalhe/portaria/273-2013-499243

Portaria n.º 372/2012, de 16 de novembro. Fixa os requisitos técnicos mínimos das câmaras fixas e portáteis de videovigilância. Diário da República n.º 222/2012: I Série de 16 de novembro. https://dre.pt/dre/detalhe/portaria/372-2012-191103

Ratcliffe, J. (2006). *Video surveillance of public places. Problem-oriented guides for police: response guides series n.º 4.* Office on Community Oriented Policing Services https://cops.usdoj.gov/ric/Publications/cops-p097-pub.pdf

Samuel, A. L. (1959). *Some studies in machine learning using the game of checkers*. IBM Journal of research and development, 3(11), 211-229 https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5392560

Security Magazine (2021). *Uma nova Era para a analítica de vídeo.* Consultado a 21 de 01 de 2023. https://www.securitymagazine.pt/2021/12/08/uma-nova-era-para-a-analitica-de-video/

Security Magazine, (2022). *Inteligência Artificial é principal tendência no mercado da videovigilância.* Consultado a 21 de 01 de 2023. https://www.securitymagazine.pt/2022/09/28/inteligencia-artificial-e-principal-tendencia-no-mercado-da-videovigilancia/

Segurança Eletrónica (2022). *O que é vídeo analítico e como ele funciona.* Consultado a 24 de 01 de 2023. https://revistasegurancaeletronica.com.br/o-que-e-video-analitico-e-como-ele-funciona/

Spicer, D. (2007). *Oral history of John McCarthy*. Computer History Museum. https://archive.computerhistory.org/resources/access/text/2012/10/102658149-05-01-acc.pdf

União Europeia. (2012). *Carta dos direitos Fundamentais da União Europeia.* Jornal Oficial da União Europeia, C326/391 https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR

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

Veiga, M. A.G.T. (2021). *Ética e adoção da inteligência artificial.* [Dissertação de mestrado não publicada]. Instituto Superior de Economia e Gestão da Universidade de Lisboa. http://hdl.handle.net/10400.5/22847

Velho, Marta. (2023, 26 de janeiro). *Primeira linha - O boom da inteligência artificial.* Jornal de Negócios. Nº4919. 5-9

Wang, P. (2019). On defining artificial intelligence. *Journal of artificial general intelligence*, 10(2), 1-37. https://doi.org/10.2478/jagi-2019-0002