INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA

VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

A Inteligência Artificial na Prevenção da Criminalidade contra o Património: Análise de experiências Europeias e oportunidades para a PSP

Auditor/a

João Miguel Pereira Silva

Lisboa, 10 de outubro de 2025

Resumo

Este trabalho avaliou de forma crítica o contributo da Inteligência Artificial para a prevenção da criminalidade contra o património na PSP, partindo do peso estrutural deste fenómeno no Relatório Anual de Segurança Interna de 2024 e das prioridades estratégicas da instituição. Com base em revisão de literatura e em relatórios técnicos, o estudo analisou duas famílias de aplicação documentadas na Europa: o policiamento preditivo baseado no espaço e tempo, exemplificado pelo Crime Anticipation System nos Países Baixos, que priorizou áreas urbanas de risco quando existiu densidade suficiente de ocorrências e validações sistemáticas; e a videovigilância algorítmica não biométrica, testada nos Jogos Olímpicos e Paralímpicos de Paris de 2024, que aumentou a deteção de intrusões e de aglomerados, mas gerou falsos positivos relevantes para alvos complexos e baixas taxas de conversão de alertas em intervenção. Concluiu-se que a Inteligência Artificial produziu ganhos operacionais quando integrada num Policiamento Orientado pela Inteligência, com supervisão humana e sendo auditada, em conformidade com legislação europeia e nacional referente à proteção de dados e à Inteligência Artificial.

Palavras-chave: Inteligência Artificial, Prevenção criminal, Criminalidade patrimonial, Policiamento preditivo, Videovigilância algorítmica.

Abstract

This study critically assessed the contribution of Artificial Intelligence to the prevention of property crime in the PSP, based on the structural weight of this phenomenon in the 2024 Annual Internal Security Report and the institution's strategic priorities. Based on a review of the literature and technical reports, the study analysed two families of applications documented in Europe: predictive policing based on space and time, exemplified by the Crime Anticipation System in the Netherlands, which prioritised urban areas at risk when there was sufficient density of incidents and systematic validations; and non-biometric algorithmic video surveillance, tested at the 2024 Olympic and Paralympic Games in Paris, which increased the detection of intrusions and clusters but generated significant false positives for complex targets and low rates of conversion of alerts into intervention. It was concluded that Artificial Intelligence produced operational gains when integrated into Intelligence-Led Policing, with human supervision and auditing, in accordance with European and national legislation on data protection and Artificial Intelligence.

Keywords: Artificial Intelligence, Crime prevention, Property crime, Predictive policing, Algorithmic video surveillance.

Índice

Introdução

A criminalidade contra o património (furtos, roubos, danos, burlas, entre outros) tem sido a categoria criminal com maior representatividade em Portugal. De acordo com o Relatório Anual de Segurança Interna (RASI) do ano de 2024, 52,4% da criminalidade participada foi referente a crimes contra o património, destacando-se, dentro destes, o crime de furto. Só o crime de furto, nas suas várias formas, representou 26% do total da criminalidade participada no ano 2024 em Portugal (RASI, 2024).

A Polícia de Segurança Pública (PSP) concentra uma parte substancial da sua atividade diária na investigação deste tipo de ilícitos criminais, em toda a sua área de responsabilidade, tentando sempre que possível, levar à justiça os suspeitos da prática destes crimes e restituir os bens furtados aos cidadãos lesados. É um desafio constante e um esforço policial quotidiano que é feito tendo em conta a pressão social, cada vez maior, por forma a que as respostas da PSP sejam o mais célere e eficazes possível, tendo a consciência que os recursos humanos são cada vez mais escassos.

Face a este panorama, a aposta na prevenção deste tipo de crime é fundamental. Pelo menos desde 2004 que a prevenção da criminalidade não organizada na União Europeia é preocupação da Comissão Europeia. É a própria Comissão Europeia a descrever este tipo de criminalidade como criminalidade de massa, que embora não organizada, ocorre com frequência, tem vítimas facilmente identificáveis e envolve frequentemente violência física, como assaltos domésticos, furtos/roubos de rua e de veículos. Refere ainda que é uma das principais preocupações das populações urbanas e inevitavelmente das Forças de Segurança (Comissão Europeia, 2004).

Ao nível interno, a Lei n.º 51/2023 de 28 de agosto, que define os objetivos, prioridades e orientações da política criminal para o biénio 2023-2025, enfatiza bem a importância da prevenção criminal. De entre o catálogo de crimes que define como crimes de prevenção prioritária (Art.º. 4º), enumera logo na alínea b) vários crimes contra o património, como furtos em viaturas, furto qualificado, roubo em residências e em edifícios comerciais ou industriais, entre outros.

Também no seio da PSP, concretamente na sua Estratégia 2025-2027, embora em sentido lato, a Prevenção é definida como um dos seis pressupostos essenciais do modelo de atuação policial, a par da Proximidade, Dissuasão, Deteção, Resposta e Adaptação, fazendo parte integrante do eixo estratégico n.º 1 - Sentimento de Segurança dos Cidadãos, especificamente na Linha Estratégica 1.2 - "Melhorar continuamente as estratégias operacionais de prevenção e combate à criminalidade…".

A necessidade constante em apostar na prevenção criminal entronca obrigatoriamente com outro eixo estratégico da PSP, o Eixo n.º 5 - Inovação e desenvolvimento. A PSP, como força de segurança com maior impacto nos centros urbanos em Portugal e por forma a responder aos constantes desafios diários e futuros, com altos padrões de eficácia e eficiência, pretende dar continuidade a um processo de "transformação digital (…) e adoção de tecnologias avançadas, como sistemas inteligentes de videovigilância e ferramentas de análise preditiva e prescritiva baseadas em inteligência artificial (IA)" (Estratégia 2025-2027 da PSP).

Neste contexto, e atendendo a que na PSP, pelo menos a nível oficial e transversalmente a todo o efetivo, é ainda bastante residual a utilização de sistemas ou ferramentas de IA, abordar-se-á de que forma a utilização destas ferramentas, acopladas à experiência adquirida pelos profissionais da PSP, poderá influenciar e melhorar significativamente o processo preventivo no que aos crimes patrimoniais respeita, principalmente os chamados na gíria como "crimes de rua".

Através da análise de casos de utilização em países europeus, tentar-se-á identificar os pontos positivos, vulnerabilidades e eventuais oportunidades de transposição para a PSP, tendo presente o equilíbrio necessário entre aproveitar o potencial da IA e a garantia de defesa de direitos, liberdades e garantias individuais.

Metodologia

O presente trabalho incide sobre a utilização de aplicações de IA por polícias europeias, que auxiliem na prevenção de crimes contra o património (furtos, roubos, vandalismo e danos em bens públicos/privados), com potencial de utilização na PSP.

Pretende-se responder à seguinte questão: Apesar do investimento crescente em tecnologias de IA por polícias europeias, em que medida as ferramentas de IA poderão contribuir para a redução efetiva da criminalidade contra o património em contexto urbano português?

A criminalidade contra o património é uma preocupação central das forças de segurança, com impacto direto na perceção de segurança dos cidadãos e na proteção dos seus bens. Com cada vez mais dificuldades no recrutamento e com a constante evolução tecnológica, a IA surge como uma ferramenta inovadora que pode simplificar processos e ser utilizada na antecipação, prevenção e investigação destes crimes, alinhando-se com as prioridades estratégicas da PSP e com as políticas europeias de segurança.

Definiram-se três objetivos para o presente estudo: identificar e analisar as principais aplicações de IA na prevenção de crimes contra o património em uso a nível europeu; avaliar resultados concretos de projetos e experiências cujo início não tenha excedido os últimos vinte anos; e, por último, propor recomendações para a implementação responsável de ferramentas de IA no contexto policial português.

A metodologia adotada baseou-se numa abordagem de estudo teórico, centrado na análise crítica da literatura científica e dos principais relatórios institucionais europeus, sobre a aplicação de ferramentas de IA na prevenção e redução da criminalidade contra o património.

A pesquisa cingiu-se a artigos científicos, documentos e relatórios da Europol e de Polícias europeias, sendo escolhidos com base na sua relevância para o tema, contexto europeu e foco em crimes patrimoniais. Outros projetos de IA aplicados a diferentes tipos de criminalidade e sem transferibilidade para a prevenção de crimes contra o património foram excluídos.

O trabalho está estruturado de forma lógica e progressiva, apresentando os conceitos-chave, enquadramento legal, a experiência de diferentes países e uma reflexão fundamentada sobre as práticas e implicações do uso da IA na prevenção da criminalidade contra o património.

1. Estado da Arte

1.1. Contextualização Teórico-Conceptual

A prevenção criminal, no quadro da Segurança Interna portuguesa, constitui-se como um dos quatro pilares da dimensão da segurança, sendo as outras três representadas pela ordem pública (repressão), informações e investigação criminal (Cabral, 2011; Oliveira, 2006).

Perante a centralidade dos furtos, roubos, dano e vandalismo urbano, do presente estudo, o enquadramento teórico-conceptual da utilização de IA como auxílio para a sua prevenção passará pela abordagem de três áreas: o conceito de prevenção criminal, a concretização do que são os modelos de policiamento Hot Spot e o orientado por inteligência/informações, e uma abordagem genérica à envolvente da "ciência dos dados", abordando tópicos como o big data, machine learning e visão computacional.

A prevenção criminal, entendida como o conjunto de estratégias destinadas a reduzir a incidência e os danos do crime antes da sua ocorrência, atua sobre oportunidades, rotinas e contextos (Clarke, 1995; Tilley, 2009). Já a prevenção situacional enfatiza a necessidade

de dificultar o acesso aos alvos, indo desde o controlo de acessos, passando pela vigilância humana ou através de sistemas tecnológicos, até à redução da recompensa ou produto final do crime, influenciando o cálculo custo/benefício do infrator (Cornish & Clarke, 2003).

Nos crimes contra o património, a evidência empírica mostra padrões espaciotemporais e fenómenos de repetição e/ou de "quase repetição", criando margem e possibilidade para uma antecipação tática do "onde" e "quando" o risco dessas práticas aumenta (Johnson et al., 2007; Townsley et al., 2003).

O policiamento Hot Spot ou policiamento de pontos quentes, é uma estratégia que pressupõe o trabalho prévio de determinar os locais, horários e tipo de crime, de maior concentração de ilícitos criminais, e com isso direcionar os meios policiais para intervenção. Esta intervenção pode passar pelo simples aumento da visibilidade policial, por intervenções do tipo "tolerância zero" direcionadas a infrações menores, por realização de operações de fiscalização policial de âmbito específico, por uma intervenção focada e direta a determinados infratores conhecidos e identificados ou, por último, por uma intervenção que realmente procure identificar as causas subjacentes ao problema de concentração de criminalidade no local e procure soluções personalizadas, em rede com outras entidades locais.

Em paralelo, o Policiamento Orientado pela Inteligência organiza ciclos de recolha-análise-difusão de informação acionável para priorizar riscos e alocar recursos a ameaças de maior impacto (Ratcliffe, 2016). Sobre esta base, o policiamento preditivo aplica modelação estatística e algoritmos para estimar a probabilidade de eventos criminais em células espaciotemporais, orientando proativamente os meios policiais e medidas de prevenção situacional (Perry et al., 2013). A vertente espacial de hotspots e não a previsão individualizada, apresenta maior maturidade empírica em crimes patrimoniais, exigindo, porém, monitorização dos ciclos de retroalimentação e enviesamentos (Lum & Isaac, 2016; Mohler et al., 2015). Esta lógica está presente em instrumentos legais europeus e nacionais, que serão tratados adiante, que balizam o tratamento de dados pelas forças de segurança, com princípios de necessidade, proporcionalidade, minimização e responsabilização que condicionam a arquitetura de qualquer solução tecnológica.

Do ponto de vista técnico, a IA designa sistemas informáticos capazes de executar tarefas que, realizadas por humanos, requereriam quesitos da sua inteligência, como a aprendizagem, o raciocínio, a resolução de problemas, a perceção e a compreensão da linguagem, a uma velocidade muito superior (Russell & Norvig, 2021; Europol, 2024). Em policiamento preventivo patrimonial, sobressaem três famílias: (1) os algoritmos estatísticos

e de aprendizagem por máquina / machine learning (ML) para a transformação de dados e informação em previsões, classificando e organizando as mesmas para a posterior tomada de decisão; (2) a visão computacional para interpretação automática de imagem/vídeo; e (3) o processamento de linguagem natural para triagem de texto e sinais.

O ML aprende padrões a partir de dados supervisionados (classificação/regressão), não supervisionadas (agrupamento/redução de dimensionalidade) e por reforço (Bishop, 2006), já o deep learning (DL), deixando de lado a intervenção humana, recorre a redes neuronais profundas para aprender padrões complexos, com ganhos notáveis em imagem/áudio, à custa de maior opacidade e exigências de dados e validação (Goodfellow et al., 2016).

Por outro lado, a visão computacional, utilizando métodos de DL específicos, permite às máquinas interpretar dados visuais e daí extrair informação que possibilita a deteção/seguimento de objetos bem como a análise de comportamentos (Szeliski, 2022). Em videovigilância, a evolução do "ver e gravar" para "ver, interpretar e alertar" concretiza-se em vídeo analítico: linhas virtuais, regiões de interesse, contagem de pessoas, deteção de objetos abandonados, fluxos anómalos e intrusões, sempre com validação humana a jusante. Na prevenção da criminalidade patrimonial, o reconhecimento de comportamentos, entendido como modelação e classificação de padrões previamente definidos, é particularmente relevante em ambientes comerciais e de retalho (Segurança Eletrónica, 2022). A legislação portuguesa atual admite sistemas de gestão analítica dos dados captados por sistemas de videovigilância, excluindo dados biométricos, sujeitando-os a descrição técnica, controlo setorial e respeito por princípios definidos em legislação específica.

O conceito de big data, definido como o conjunto de dados muito volumosos, gerados e atualizados a grande velocidade e com grande variedade de formatos, que exigem novas formas de armazenamento e análise para extrair valor e apoiar decisões (Kitchin, 2014), é essencial em ferramentas de IA, cujo propósito é a análise e treino através de dados, no entanto, além das potencialidades inerentes é também uma provável fonte de riscos. Por forma a minimizar os riscos, qualquer que seja o big data a utilizar, deve-se explicitar claramente as finalidades e base legal da sua constituição, assegurar a qualidade e representatividade dos dados a analisar, documentar as origens dos dados e estabelecer controlos de acesso e de auditoria.

No plano da validação, três desafios estruturam a adoção responsável de IA no policiamento. Primeiro, a validade e a generalização. Modelos treinados num contexto podem degradar noutro, impondo-se aqui validações externas, testes e avaliações antes e

depois da sua implementação, com métricas como sensibilidade, precisão, tempo para deteção e custo-benefício (Hand, 2006; Perry et al., 2013). Segundo, a sua explicabilidade e supervisão. Decisões que interferem com direitos, liberdades e garantias de cidadãos bem como a alocação de meios públicos, devem ser escrutináveis, com modelos transparentes e explicáveis quando necessário, mantendo a intervenção humana como imprescindível e a possibilidade de auditoria (Doshi-Velez & Kim, 2017; Ribeiro et al., 2016). Em terceiro, a justiça algorítmica, ética e viés. Desde a escolha de variáveis à classificação de dados podem-se reproduzir desigualdades e daí originar a concentração excessiva de policiamento em determinados locais. Exige-se por isso uma constante monitorização de erros, definição de limites operacionais e avaliações de impacto habilitantes à decisão de manutenção ou redistribuição de efetivos (Lum & Isaac, 2016; Barabas et al., 2018). A experiência europeia recente de videovigilância algorítmica em grandes eventos, como veremos adiante, ilustra ganhos de perceção situacional em intrusões e gestão de densidades, mas também taxas relevantes de falsos positivos para alvos complexos (p. ex., chamas/armas) e necessidade de métricas de desempenho robustas antes de generalizações (Comité de Avaliação, 2025).

Feito o genérico mas necessário enquadramento de conceitos e teoria relacionados com o tema, seguiremos agora para a necessária análise legal, ao nível europeu e nacional.

1.2. Quadro jurídico-ético na adoção de ferramentas de IA na prevenção criminal

A crescente evolução tecnológica bem como disseminação mundial de ferramentas de IA, algumas delas completamente gratuitas e de livre utilização, teve de ser acompanhada de normativos legais capazes de regulamentar a sua utilização. Nessa senda, a utilização de dados pessoais bem como questões éticas e morais vão surgindo, levando a que sistematicamente estas matérias sejam abordadas e discutidas.

Mesmo antes do surgimento de legislação europeia e nacional específica sobre estas matérias, temos obrigatoriamente que visitar a Constituição da República Portuguesa (CRP) e verificar os vários limites impostos naquilo que pode ser a adoção de sistemas de IA pela polícia.

Em primeiro lugar e transversal a toda a atuação policial é necessário encontrar o equilíbrio entre os vários direitos, liberdades e garantias com o direito à segurança (art. 27º da CRP). Depois, direcionando-nos para algumas das questões mais sensíveis ao nível da IA, é necessário ter sempre presente o respeito pelo direito à reserva da intimidade da vida privada e familiar (art. 26º, nº 1, da CRP), à inviolabilidade do domicílio e da correspondência (art. 34º da CRP), a proteção de dados e da vida privada (art. 35º da CRP)

e a nulidade das provas obtidas com intromissões abusivas na vida privada (art. 32º, n.º 8, da CRP). Genericamente, devem-se respeitar os princípios de um Estado de Direito, tais como a aplicação estrita da legalidade e a proteção de dados (Canotilho, 2003). Estes preceitos impõem a necessidade, proporcionalidade e adequação de quaisquer meios técnicos usados na prevenção do crime, mas também na investigação dos mesmos, sob pena de inutilizabilidade da prova obtida por via ilícita.

Após a necessária alusão à CRP, é fundamental a referência aos dois regimes que surgiram na União Europeia em 2016, o Regulamento (UE) 2016/679 (RGPD) e a Diretiva (UE) 2016/680, e que tiveram a sua execução e transposição para a ordem jurídica portuguesa em 2019, na Lei n.º 58/2019 e na Lei n.º 59/2019, ambas de 8 de agosto, respetivamente.

O primeiro normativo, o Regulamento Geral de Proteção de Dados (RGPD), como o próprio nome indica, tem um âmbito de aplicação generalista no que concerne ao tratamento de dados pessoais, do qual ressalvamos os princípios fundamentais descritos no seu art. 5º: a licitude, lealdade e transparência (o titular dos dados deve ser devidamente informado da recolha dos seus dados e para que fim se destinam, consentindo com tal ato); a limitação das finalidades (o uso dos dados deve ser para os fins específicos e que foram previamente informados ao seu titular); a minimização (a recolha dos dados deve cingir-se ao estritamente necessário para os fins a que se destina); exatidão (manter os dados corretos e atualizados); a limitação da conservação (guardar os dados apenas pelo tempo indispensável e necessário ao fim da sua recolha); a integridade e confidencialidade (deve ser garantida a segurança dos dados contra acessos, tratamentos não autorizados ou até mesmo contra a sua eliminação acidental); e responsabilidade, impondo ao responsável a demonstração do cumprimento de todos os princípios anteriores (Regulamento (UE) 679/2016, 2016).

Por sua vez, a Diretiva (UE) 2016/680, é apenas aplicável ao tratamento de dados por autoridades competentes para fins de prevenção, deteção, investigação ou repressão de infrações penais e execução de sanções penais, sendo muito mais setorial e restritiva. Esta Diretiva assenta em princípios próximos dos do RGPD, mas adaptados ao contexto policial. Em Portugal, a sua transposição pela Lei n.º 59/2019, de 8 de agosto, articula-se com o RGPD e a Lei n.º 58/2019, de 8 de agosto, oferecendo às forças e serviços de segurança um regime setorial que concilia eficácia operacional com a proteção dos direitos fundamentais e a prova processualmente válida.

Chegados aqui, julga-se pertinente fazer ainda uma breve referência à execução do RGPD para o ordenamento jurídico português, através da Lei 58/2019 de 8 de agosto, bem como a transposição da Diretiva (UE) 2016/680, através da Lei 59/2019 de 8 de agosto.

A Lei n.º 58/2019 de 8 de agosto, para além de assegurar a execução do RGPD na ordem jurídica portuguesa, define como autoridade de controlo nacional para efeitos desse regulamento a Comissão Nacional de Proteção de Dados (CNPD). É igualmente nesta Lei que é operacionalizada a obrigação de realização de Avaliações de Impacto de determinados tratamentos de dados (constantes de lista a ser disponibilizada pela CNPD), conforme previsto no art. 35º, n.º 4 do RGPD, bem como a definição e publicitação de outra listagem, onde constem os tipos de tratamento de dados que cuja avaliação prévia de impacto não é obrigatória.

Já na Lei n.º 59/2019 de 8 de agosto, é prevista a realização de avaliação de impacto sempre que determinado tipo de tratamento de dados seja suscetível de representar um elevado risco para os direitos, liberdades e garantias das pessoas (art. 29º) e obriga a realização de consulta prévia à CNPD antes de proceder ao tratamento efetivo dos dados (art. 30º). Também a segurança no tratamento dos dados e o registo/controlo de acesso aos mesmos é condição prevista no art. 31º do mesmo diploma.

Outro normativo legal bastante importante para o presente trabalho é a Lei n.º 95/2021, de 29 de dezembro, a qual veio revogar a Lei n.º 1/2005, de 10 de janeiro. O primeiro normativo, para a instalação e utilização de sistemas de vigilância por câmaras de vídeo pelas Forças e Serviços de Segurança (FSS), obrigava a um Parecer favorável e vinculativo por parte da CNPD. A argumentação constante dos pedidos era de tal forma questionada pela CNPD, entidade cuja função era mesmo garantir o equilíbrio entre os direitos fundamentais e a segurança, que se tornou bastante complexo e difícil de justificar a proporcionalidade e adequação do uso destes sistemas (Frois, 2015). Com a entrada em vigor da Lei n.º 95/2021, de 29 de dezembro surgiram alterações significativas. Uma mudança relevante foi a eliminação do caráter vinculativo do parecer da CNPD na validação de sistemas de videovigilância, que apesar de continuar a ser necessário não é vinculador, cabendo agora ao membro do Governo que tutela a força ou serviço de segurança a autorização de instalação do sistema. No art. 3º, passou a incluir-se a prevenção de atos terroristas, fundamento que antes não constava. O prazo máximo da autorização é agora de três anos, ao contrário dos anteriores dois anos, renovável por período igual ou inferior (art. 7º, n.º 2). De relevo para o tema do trabalho apontamos a admissibilidade da utilização de sistemas de gestão analítica dos dados captados, desde que o pedido inicial inclua a descrição

técnica do sistema de IA (art. 6º, n.º 1, alínea g)). Finalmente, o diploma vem permitir a recolha e o tratamento de dados, à exceção dos dados biométricos (art. 16.º).

Em 2024, a União Europeia aprovou o Regulamento (UE) 1689/2024 (Regulamento Europeu sobre IA) que consagra de forma expressa uma abordagem baseada no risco. Desde estabelecer a proibição de determinadas práticas de IA (art. 5º), passando pela classificação de alguns sistemas de IA como sendo de risco elevado (art. 6º), e inerente a tal acionando um conjunto exigente de obrigações, previstas entre os artigos 9º a 15º, o diploma impõe requisitos técnicos e organizativos rigorosos, como a gestão de risco estruturada, padrões elevados de qualidade dos dados, mecanismos robustos de cibersegurança, supervisão humana clara e a possibilidade de auditorias para verificação desse cumprimento (Regulamento (UE) 1689/2024).

Analisados os principais diplomas legais com implicação em contexto de tratamento de dados, importa referir que qualquer que seja a ferramenta com IA a implementar por forma a auxiliar na prevenção de crimes contra o património a mesma deve respeitar, de forma rigorosa, os preceitos estabelecidos nos diplomas legais atrás referidos. Para além do quadro jurídico, é crucial garantir o respeito por princípios éticos basilares, entre eles, evitar ao máximo danos para terceiros garantindo a segurança dos dados, prevenir a discriminação, assegurar a supervisão humana e promover transparência e explicabilidade nos processos automatizados. Só uma abordagem que una conformidade legal e responsabilidade ética permitirá que a introdução de soluções de IA aumente a eficiência operacional sem pôr em causa os direitos, liberdades e garantias dos cidadãos.

2. Experiências documentadas de Polícias Europeias

Após o necessário enquadramento conceptual da envolvente à implementação de ferramentas de IA à prevenção criminal, em especial dos crimes contra o património, bem como a pequena análise jurídica ao nível europeu e nacional, passaremos agora a identificar e descrever as experiências europeias selecionadas tendo por base a metodologia adotada e as limitações do presente trabalho. De entre a empregabilidade conhecida de ferramentas de IA na atividade policial, pela pesquisa efetuada, para efeitos de utilização e auxílio em prevenção criminal contra crimes patrimoniais de rua (furtos, roubos, danos), verificou-se que apenas o Policiamento Preditivo e a Videovigilância são áreas onde realmente esta tecnologia foi implementada e testada. Como tal, a abordagem do presente capítulo incidirá precisamente nestas duas aplicações.

2.1. Policiamento Preditivo com IA

Em 2022, a European Crime Prevention Network (EUCPN), esclarece que a polícia preditiva é atualmente utilizada em vários departamentos policiais europeus, incluindo os Países Baixos, Alemanha, Áustria, França, Estónia e Roménia. Atualmente, o Policiamento Preditivo é usado principalmente para prevenir alguma da criminalidade contra o património (alguns furtos e roubos). Neste domínio, os Países Baixos são considerados pioneiros, uma vez que foram o primeiro país do mundo a implementar o policiamento preditivo à escala nacional, através do seu *Crime Anticipation System* (CAS) (Willems, 2017; Mali et al., 2017).

Na Alemanha, a ferramenta preditiva PRECOBS visa principalmente os roubos em residências, utilizando dados históricos dos últimos cinco anos. A Áustria e a França utilizam o policiamento preditivo para antecipar roubos/furtos em residências e de veículos. Na Áustria são utilizados dados históricos sobre crimes (tipo de crime, hora, local, modus operandi e informações sobre o local) e em França, os dados introduzidos baseiam-se nas queixas apresentadas, estatísticas criminais e geolocalizações de crimes de roubo e furto de automóveis dos últimos sete a dez anos. A Estónia utiliza o policiamento preditivo para prever crimes baseando-se em eventos, áreas e pessoas, através da análise de dados criminais, dados relacionados com as passagens de fronteiras e até dados acerca de mortes não naturais (relacionadas com drogas, acidentes de trânsito e homicídios). A Roménia utiliza o policiamento preditivo para prever crimes baseados em áreas e pessoas (EUCPN, 2022).

Face ao leque de países mencionados com utilização de Policiamento Preditivo, optou-se por abordar mais a detalhe a ferramenta utilizada na realidade dos Países Baixos, o CAS, visto ter sido pioneiro na sua implementação a nível nacional e devido ao destaque em publicação recente da EUROPOL - AI and Policing - The benefits and challenges of artificial intelligence for law enforcement (2024).

2.1.1. Crime Anticipation System (CAS) – Países Baixos

O CAS é um sistema algorítmico de previsão no espaço e no tempo do crime, que gera previsões a partir de dados, que assenta em métodos estatísticos e mineração de dados. Assim, à luz do Regulamento (UE) 1689/2024, enquadra-se na definição de sistema de IA, motivo pelo qual o abordamos o mais detalhadamente possível perante a bibliografia disponível.

O Sistema de Antecipação de Crime (tradução do autor) foi desenvolvido pela Polícia de Amesterdão, dos Países Baixos, num contexto de transição para um modelo de Policiamento orientado pela inteligência e na criação de uma base nacional padronizada de informação criminal. Em termos operacionais, o CAS procura antecipar a ocorrência de crimes com base em análise estatística por IA, proveniente de três fontes de dados: Base de Informação Policial, Bases de dados Municipais das cartografias e Bases de dados/indicadores demográficos. (Willems & Doeleman, 2014; Willems, 2017; Mali et al., 2017).

Trata-se de um sistema preditivo espaciotemporal, focado em zonas e horários críticos para a ocorrência de crimes contra o património, considerados pela Polícia dos Países Baixos como de elevado impacto (p. ex., furtos e roubos na via pública, furtos em residência), não visando a questão individualizada de qualquer tipo de perfil de suspeito. O território urbano é segmentado numa grelha de 125×125m e apenas os 3% de células com risco mais elevado são realçados, sob a forma de mapas de calor, ajustando a previsão à capacidade de patrulhamento disponível (Willems, 2017; Mali et al., 2017).

O sistema teve uma versão em 2015, na qual o algoritmo considerava ocorrências em períodos quinzenais e mensais e dois coeficientes direcionais, e outra em 2017, onde optaram por passar para uma periodicidade semanal, com 12 semanas consecutivas e um único coeficiente direcional (Willems, 2017).

Em termos de implantação, após os testes em Amesterdão, seguiram-se experiências piloto noutras cidades dos Países Baixos, sendo que em maio de 2017 o CAS foi disponibilizado a toda a polícia do País (Willems, 2017; Mali et al., 2017).

Entre as mais valias identificadas, salientam-se a padronização e automatização, visto que os mapas são gerados de forma automática e acessíveis via web simples, reduzindo o esforço técnico dos utilizadores finais; a possibilidade de melhor orientação tática, atendendo a que as previsões servem para melhor orientar o "quando" e "onde" direcionar o policiamento; e, face à alteração de 2017, atendendo a que se tratam de ambientes urbanos e o número de ocorrências é suficiente para ter impacto estatístico, o aumento da resolução temporal e espacial, que aumentou a qualidade das previsões. Em ambientes urbanos com muitas ocorrências, esta combinação aumenta a qualidade das previsões, por outro lado, em áreas com poucas ocorrências, o ganho de resolução não se traduz automaticamente em melhor previsão. (Willems, 2017; Mali et al., 2017).

Contudo, a literatura e a análise crítica destacam algumas limitações e riscos. Em primeiro lugar, limitações metodológicas, isto é, o CAS é adequado sobretudo a fenómenos

criminais com forte ligação a determinado espaço, tempo e frequência suficiente (furtos, roubos, furtos por carteiristas), sendo pouco indicado para outro tipo de crimes mais raros (homicídio) ou menos participados (violência sexual) bem como para crimes que não se consegue desde logo determinar a sua origem (burlas informáticas) (Oosterloo & Van Schie, 2018). Além disso, a delimitação temporal de certos crimes (p. ex., furto em residência) recorre frequentemente a "meios-dias" por incerteza da hora exata, o que pode distorcer gráficos de "horas de risco" (Willems, 2017; Oosterloo & Van Schie, 2018).

Em segundo lugar, nas opções de categorização, concretamente na versão de 2015, era incluído um indicador com o número de "alóctones não-ocidentais" por área de código postal, que foi removido em 2017 por "não acrescentar valor preditivo" (Willems, 2017). Ainda neste indicador, a mera distinção estatística de "ocidental/não-ocidental" reflete por si só uma questão com potencial para introduzir vieses étnico-raciais (Oosterloo & Van Schie, 2018).

Como terceiro risco, é apontado o facto de o sistema parecer ter uma espécie de "caixa negra organizacional", isto é, apesar do CAS apresentar visualmente os mapas de risco e as linhas temporais, quem visualiza tem acesso limitado aos dados que os originaram, o que pode levar à tomada de decisões baseadas apenas na camada visual, sem qualquer outra contextualização ou apoio para a decisão. Esta dinâmica da tomada de decisão baseada apenas no que se visualiza através de um mapa ou gráfico, juntamente com vieses humanos originários do policiamento de 1.ª linha, pode alimentar "ciclos de retroalimentação", o que gera desvantagens significativas para determinados grupos populacionais e áreas de responsabilidade (Oosterloo & Van Schie, 2018).

Em suma, o CAS constitui-se como uma ferramenta de apoio à decisão, mais precisamente no direcionamento do policiamento. É um instrumento automatizado e padronizado, com provas dadas em Amesterdão. Como vantagens garante uma rápida apresentação gráfica ao decisor, permitindo ao mesmo orientar e direcionar da melhor forma o policiamento na sua área de responsabilidade. Como limitações, é um sistema que funciona apenas para tipos específicos de crime, devido à especificidade de determinar concretamente o horário de ocorrência do crime bem como a própria incidência desse tipo de crime em determinado local. Apresenta igualmente alguns riscos de viés nos dados e ao nível da interpretação apenas permite a visualização do resultado final do sistema, inibindo uma análise mais detalhada. Estas limitações exigem claramente uma boa gestão de dados, auditorias contínuas e práticas de validação no terreno, por forma a assegurar

proporcionalidade e equidade (Willems, 2017; Oosterloo & Van Schie, 2018; Schuilenburg & Soudijn, 2023).

2.2. Videovigilância com IA

Nos últimos anos, a videovigilância evoluiu no sentido de integrar a captação de imagens com a sua análise automática, permitindo gerar alertas e, desse modo, potenciar intervenções de segurança (Security Magazine, 2021), ao invés dos antigos sistemas que se limitavam a captar e gravar as imagens sem qualquer outra funcionalidade em tempo real.

Conforme Frois (2011), que recupera uma intervenção do então Ministro da Administração Interna, Rui Pereira (2007), as sociedades atuais, marcadas pela globalização, configuram-se como sociedades de risco, em que as ameaças ganham novas expressões e amplitudes. Face a esse contexto, impõe-se uma resposta inovadora que capitalize as novas tecnologias, destacando-se os sistemas de videovigilância, os quais, "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).

Nesta senda, ao acoplar sistemas de IA à videovigilância de modo a que mesma não só capte e armazene vídeo, mas que interprete automaticamente essas imagens e acione alertas para posterior validação e tomada de decisão humana, entramos no ramo do vídeo analítico. São várias as capacidades de uma tecnologia de vídeo analítico, desde a tecnologia termográfica, a deteção de objetos específicos, o cruzamento de linhas virtuais, regiões de interesse, o sentido de movimento, o reconhecimento de comportamentos, contagens de pessoas, o rastreamento dessas pessoas na imagem e o reconhecimento facial (Security Magazine, 2022; Segurança Eletrónica, 2022).

Entre as funcionalidades do vídeo analítico, o reconhecimento de comportamentos é provavelmente a mais relevante para a prevenção da criminalidade patrimonial. Esta capacidade assenta na modelação e classificação de padrões comportamentais previamente definidos, permitindo aos algoritmos associar diferentes sequências de movimento ao mesmo comportamento/alvo e gerar alertas operacionais. Na prática, é amplamente usado em centros comerciais e lojas, para sinalizar ocorrências de potenciais furtos, roubos, agressões ou vandalismo, bem como incidentes como quedas ou acidentes. (Segurança Eletrónica, 2022).

Feito o enquadramento sobre a aplicação da IA num sistema de videovigilância e mencionada a funcionalidade que mais se adequará à prevenção da chamada "criminalidade de rua" abordaremos de seguida o caso prático da utilização do sistema de videovigilância

com algorítmica específica aquando da realização dos últimos Jogos Olímpicos, em 2024, em Paris.

2.2.1. Sistema de Videovigilância Algorítmica - Vídeosurveillance Algorithmique (VSA) – Polícia de Paris

Em França, após um processo legislativo interno habilitante em 2023, foi implementado um regime experimental e temporário para a utilização de algoritmos associados às câmaras de videovigilância e a drones, com vista à deteção em tempo real de "eventos predeterminados" em grandes eventos, excluindo expressamente o reconhecimento facial.

Esta tecnologia, chamada de videovigilância algorítmica (VSA), usada pela Police Nationale em Paris 2024, no decorrer dos Jogos Olímpicos, consistiu em acoplar analítica por IA às câmaras existentes, com o intuito de detetar padrões, comportamentos de risco ou possíveis vulnerabilidades em tempo real. Concretizando, a função específica desta tecnologia seria a deteção em áreas proibidas no perímetro dos Jogos Olímpicos de Paris do seguinte: objetos abandonados, presença ou uso de armas, veículos a circular em sentido oposto ao permitido, intrusão ou presença em zonas proibidas ou consideradas sensíveis, pessoas no chão (por queda ou doença súbita), movimentos de multidões, aglomerados excessivos de pessoas e indícios de incêndio.

O sistema não foi capacitado para a identificação de pessoas, mas sim para funcionar como detetor de eventos e comportamentos para posterior sinalização a um operador, mantendo-se a decisão final no controlo humano. A ideia principal era ganhar tempo através da deteção precoce de situações potencialmente perigosas e priorizar a resposta policial em contextos de grande afluência (Zatsepina & Ludvigsen, 2025).

Os Jogos Olímpicos de Paris 2024 serviram como um "mega evento laboratório". Foram usados para testar e legitimar estas tecnologias em condições reais de operação, com forte atenção pública e mediática, originando tensões entre a eficácia operacional e os direitos fundamentais das pessoas (Zatsepina & Ludvigsen, 2025).

Em termos práticos, foi integrado software de analítica de vídeo em centros de comando e em redes de transportes públicos, calibrando regras para acontecimentos predefinidos e afinando a alarmística (p. ex., densidade ou fluxo acima do esperado). O objetivo tático era elevar a consciência situacional em tempo real e reduzir o tempo de verificação até um primeiro olhar humano, isto é, não seria propriamente prever crimes, mas sim antecipar cenários de risco antes de escalarem (Zatsepina & Ludvigsen, 2025).

Das evidências académicas e das sínteses públicas de avaliação da utilização deste sistema extraímos um balanço misto entre os aspetos positivos e negativos. O Comité de Avaliação apresentou, em inícios de 2025, um balanço mitigado acerca do sistema. Por um lado, revelou ser bastante eficaz na deteção de casos de intrusão de pessoas em zonas proibidas/interditas e em gestão de excessos de densidade de pessoas/movimentos de multidão, por outro, não se mostrou tão útil na deteção por exemplo de chamas, armas, objetos abandonados, apresentando muitos falsos casos positivos (incluindo confusão entre pessoas em situação de sem abrigo e objetos abandonados). O número total de intervenções no terreno geradas pelos alertas foi baixo, no entanto as entidades ressalvam que a eficácia não se mede apenas por intervenções, mas também por melhor consciência situacional e priorização (Comité de Avaliação, 2025).

Entre os resultados positivos foram destacados a melhoria da perceção situacional nas salas de operações, com alertas a ajudarem os operadores a detetar intrusões e picos de densidade mais cedo, facilitando a gestão de fluxos em zonas críticas; a integração procedimental de registo e validação humana, que permitiu a redução do risco de decisões automatizadas sem escrutínio e, a utilidade operacional percecionada pelo operadores, já que os próprios referiram terem tido ganhos pontuais em rapidez de triagem, sobretudo em ocorrências espaciais/contextuais e não centradas em indivíduos (Comité de Avaliação, 2025; Zatsepina & Ludvigsen, 2025).

Relativamente aos aspetos negativos e limitações, foram apontadas questões relacionadas com o posicionamento das câmaras e alguma imaturidade tecnológica no que concerne à deteção de chamas e armas, as quais acabaram por reduzir o desempenho em certos cenários. Também a ocorrência de vários falsos alertas positivos e a necessidade de confirmar muitos deles acabou por sobrecarregar algumas equipas, anulando assim o ganho de tempo que se pretendia com esta tecnologia. Associado a este último, foi também apontado negativamente a baixa convertibilidade de alertas em intervenções reais e a não apresentação de provas robustas de eficácia, subsistindo dúvidas quanto às métricas utilizadas na avaliação (Comité de Avaliação, 2025; Zatsepina & Ludvigsen, 2025; Le Monde, 2025; Pérez-Lagos & Ghassemi, 2025; Reuters, 2024).

Em síntese, a experiência francesa mostrou que a VSA tem potencial para detetar precocemente situações de risco não biométricas (intrusões, excesso de pessoas em determinado espaço), com validação humana e enquadramento jurídico dedicado. No entanto, revela também limitações técnicas, nomeadamente vários falsos alertas positivos

bem como a necessidade de definição de métricas de avaliação de desempenho claras e objetivas antes de qualquer generalização.

Discussão e oportunidades para a PSP

Os resultados sintetizados neste trabalho refletem que as aplicações de IA com maior maturidade e utilidade operacional na prevenção da criminalidade contra o património são as abordagens espaciotemporais (hotspots) de policiamento preditivo e a videovigilância com analítica não biométrica, mas focada para o reconhecimento de comportamentos de preparação para a prática de ilícito criminal ou de oportunidades para a prática dos mesmos. Em ambas as aplicações, observam-se ganhos significativos para um decisor. Seja na perspetiva de um Comandante de Esquadra, pois conseguiria ter uma maior consciência situacional do que vai acontecendo na sua área de responsabilidade, com regular atualização, e que lhe permitiria projetar e direcionar os seus meios de policiamento para zonas identificadas, garantindo que as suas decisões seriam oportunas e sustentadas. Seja igualmente na posição de Operador/Supervisor de sistemas de videovigilância numa central da PSP, cujo acionamento de meios para confirmação de determinada alarmística ou intervenção, originada por uma câmara, seria sempre antecipada da sua análise em tempo real, funcionando como um filtro mas também como um ganho de tempo relativamente à eventual ocorrência do ilícito criminal.

Foram percecionados igualmente alguns limites metodológicos e riscos de enviesamento de resultados, impostos por normativos legais, princípios éticos e questões operacionais (Perry et al., 2013; Lum & Isaac, 2016). Esta leitura é coerente com os objetivos e o escopo definidos para o estudo, centrados em crimes de rua e de elevada repetição (furtos, roubos, dano/vandalismo), bem como com a estratégia de transformação digital da PSP e respetivo enfoque em videovigilância inteligente e análise preditiva (Direção Nacional da PSP, 2025).

No caso do policiamento preditivo, a experiência CAS confirma a vantagem de modelos orientados por "lugar e tempo", aplicados a fenómenos com forte regularidade espaciotemporal. A grelha de 125×125 m e a seleção dos 3% de células de maior risco, alinhadas com a capacidade de patrulhamento, traduzem-se em automatização e padronização úteis para a decisão operacional (Willems, 2017; Mali et al., 2017). Esta constatação converge com a evidência de campo de Mohler et al. (2015), que, em ensaios controlados aleatórios, observaram melhorias na alocação de patrulhas e, nalguns contextos, reduções localizadas de ocorrências. Contudo, este sistema revela ser bastante dependente

da densidade de ocorrências, em que os ganhos de resolução temporal e espacial elevam a qualidade preditiva em centros urbanos, mas pouco acrescentam onde os dados são escassos (Willems, 2017; Mali et al., 2017).

Outro fator a considerar é a escolha das variáveis e indicadores potencialmente geradoras de viés. O estudo de indicadores com real valor preditivo deve ser assegurado (Willems, 2017) e adotado, mantendo padrões éticos e legais. Também a explicabilidade dos resultados é necessária, ter acesso aos dados e perceber como se chegou a determinado mapa de calor. Para além disso, é tão importante como se usa o mapa como o quanto o mapa mostra, para tal, é necessária a validação do algoritmo com base em métricas definidas pós utilização (Ratcliffe, 2016; Schuilenburg & Soudijn, 2023).

Ainda na lógica de transposição para a PSP, afigura-se necessário ressalvar que um sistema destes deverá ser configurado de forma diferente perante as diferenças existentes entre os vários Comandos de Polícia. A densidade de ocorrências de furtos/roubos/danos é necessariamente diferente em diversas áreas da responsabilidade da PSP, como tal são necessários ajustes por forma a apresentar os resultados desejáveis.

Nos sistemas de videovigilância com analítica, a experiência francesa de VSA em Paris 2024 clarifica um ponto crucial, quando o objetivo é detetar eventos/comportamentos e não a identificação de indivíduos, a IA acrescenta velocidade de triagem e ganho de consciência situacional, desde que a calibração de regras seja a correta e a validação humana imediata. Os balanços públicos indicam eficácia em intrusões e gestão de densidades, mas desempenho fraco e com muitos falsos positivos em alvos complexos (chamas, armas, objetos abandonados), com baixa convertibilidade de alertas em intervenções e sobrecarga de operadores em determinadas fases (Comité de Avaliação, 2025; Zatsepina & Ludvigsen, 2025; Le Monde, 2024, 2025).

Comparando policiamento preditivo e VSA, o primeiro atua a montante, orientando presença e dissuasão em janelas de maior risco, a segunda opera em tempo real, encurtando o tempo até à primeira análise humana. Consideramos que os dois acabam por se complementar, os mapas de risco podem informar o onde e quando intensificar vigilância e que regras algorítmicas priorizar, já os alertas de VSA, alimentam bases de incidência e características contextuais úteis para a intervenção futura (Perry et al., 2013; Johnson et al., 2007). A diferença maior reside na transferibilidade, pois neste caso não se trata apenas de calibração de parâmetros, no caso de VSA, o sucesso está muito dependente das características das câmaras, ângulos e dinâmicas das pessoas, exige adaptação frequente por local e evento (Comité de Avaliação, 2025; Szeliski, 2022).

Do ponto de vista legal e ético, verifica-se a necessidade do cumprimento dos vários princípios definidos pelo RGPD e a Lei n.º 58/2019, sendo certa a adaptação obrigatória às exigências mais concretas impostas pela Lei n.º 59/2019. Já a Lei n.º 95/2021 admitindo a analítica em videovigilância, excluindo dados biométricos, constitui-se como uma janela de oportunidade para o desenvolvimento de algoritmos cada vez mais profícuos na deteção de movimentos e comportamentos indiciadores de atos preparatórios para a prática de ilícitos contra o património.

Os casos analisados indicam que a IA não será uma solução milagrosa, mas irá certamente libertar capacidade humana e melhorar o tempo da tomada de decisão. Para a PSP, considera-se que o caminho passará pela adoção destas duas ferramentas de IA, a operar em conjunto num projeto piloto, numa área de responsabilidade com índices de criminalidade patrimonial elevados (circunscrita eventualmente a um concelho do Distrito de Lisboa), com supervisão humana qualificada, transparência interna (guias de uso e de interpretação de mapas/alertas) e sujeitas a auditorias independentes periódicas. Só assim se maximizará o benefício operacional sem comprometer os direitos fundamentais das pessoas.

Da análise efetuada, diríamos que há oportunidades reais de ganho para a PSP, sobretudo na combinação de um Modelo de Policiamento orientado por inteligência com mapas de hotspots e ainda com videovigilância analítica não biométrica, desde que ancoradas em métricas claras, gestão de dados rigorosa e com constante supervisão humana. A literatura e os casos analisados convergem no mesmo ponto, a IA pode tornar a prevenção patrimonial mais focada, rápida e auditável. O que determinará o sucesso não é a sofisticação do algoritmo, mas a qualidade do design institucional que o envolve (Perry et al., 2013; Lum & Isaac, 2016; Schuilenburg & Soudijn, 2023; Comité de Avaliação, 2025; Zatsepina & Ludvigsen, 2025).

Conclusão

A análise realizada demonstra que a IA pode acrescentar valor à prevenção da criminalidade contra o património quando integrada num ecossistema policial maduro, isto é, com dados de qualidade, objetivos operacionais claros e mecanismos de supervisão robustos.

Os resultados convergem em três ideias principais. Primeiro, o ganho não reside na "magia" do algoritmo, mas na sua capacidade de transformar dados dispersos em prioridades operacionais, como orientar o policiamento para hotspots, antecipar janelas espaciotemporais de risco e elevar a consciência situacional através de vídeo analítico não biométrico com validação humana. Segundo, a eficácia é indissociável da legitimidade. O RGPD, a Lei 58/2019 e Lei 59/2019 ambas de 8 de agosto, a Lei 95/2021 e o Regulamento Europeu de IA impõem um caminho de responsabilidade que, longe de travar a inovação, pretende estruturar e proteger a decisão policial. Terceiro, teremos que ver a IA como um catalisador e não o substituto, dos modelos de policiamento em utilização na PSP. A IA pode melhorar a recolha, a análise e a difusão mais oportuna da informação, mas não eliminará a necessidade de interpretação e juízo humano para a tomada de decisão.

Em síntese, a PSP pode captar ganhos de eficácia e eficiência se tratar a IA como tecnologia habilitadora de um ciclo preventivo mais informado, mensurável e audível, ancorado em salvaguardas legais e éticas. O caminho responsável passará pela implementação de projetos piloto circunscritos e sua posterior avaliação interna e independente, com recolha de aprendizagens para correções subsequentes. Para além de se propor uma investigação futura acerca da demonstração causal do impacto da implementação de um destes eventuais projetos piloto, sugere-se ainda a criação de protocolos de colaboração entre a PSP e ensino superior da área tecnológica no sentido de apostar no desenvolvimento de ferramentas de IA com o propósito da segurança interna.

Bibliografia

Barabas, C., Dinakar, K., Ito, J., Virza, M., & Zittrain, J. (2018). Interventions over Predictions: Reframing the Ethical Debate for Actuarial Risk Assessment. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency, in Proceedings of Machine Learning Research.* https://proceedings.mlr.press/v81/barabas18a.html

Bishop, C. (2006). Pattern Recognition and Machine Learning. *Springer*. https://www.microsoft.com/en-us/research/wp-content/uploads/2006/01/Bishop-Pattern-Recognition-and-Machine-Learning-2006.pdf

Cabral, J. A. H. S. (2011). Do direito à segurança à segurança do Direito. Intervenção na 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/2022/09/macaufaculdadedireito.pdf

Canotilho, J. J. G. (2003). *Direito constitucional e teoria da constituição* (7ª ed.). Coimbra. Almedina.

Clarke, R. V. (1995). Situational Crime Prevention. Crime and Justice. 19. (pp. 91-150). https://doi.org/10.1086/449230

Comissão Europeia. (2004). Comunicação da Comissão ao Conselho e ao Parlamento Europeu: Prevenção da criminalidade na União Europeia. COM(2004) 165 final. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:52004DC0165

Comité de Avaliação. (2025). Rapport du Comite d'evaluation de l'expérimentation de traitements algorithmiques d'images légalement collectées au moyen de systemes de videoprotection. *Vie Publique*. https://www.vie-publique.fr/rapport/297322-experimentation-traitements-algorithmiques-dimages-de-videoprotection

Constituição da República Portuguesa (versão consolidada). (1976/2025). Diário da República. https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-aprovacao-constituicao/1976-34520775

Cornish, D., & Clarke, R. V. (2003). Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention. 16. (pp. 41-96). *Crime Prevention Studies.*

Direção Nacional da Polícia de Segurança Pública. (2025). Estratégia 2025-2027 da Polícia de Segurança Pública.

Diretiva (UE) n.º 680/2016 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. (2016). *Jornal Oficial da União Europeia*, L 119, 89–131. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016L0680

Doshi-Velez, F., & Kim, B. (2017). Towards a rigorous science of interpretable ML. https://doi.org/10.48550/arXiv.1702.08608

European Crime Prevention Network (EUCPN). (2022). Artificial Intelligence and predictive policing: risks and challenges. https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf

European Union Agency for Law Enforcement Cooperation (Europol). (2024). AI and policing: The benefits and challenges of artificial intelligence for law enforcement (Europol Innovation Lab observatory report). *Publications Office of the European Union*. https://doi.org/10.2813/0321023

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*. (pp. 222-234) Centro de Estudos Internacionais sobre Governo. Editora UFRGS. https://lume.ufrgs.br/bitstream/handle/10183/213251/001114121.pdf?sequence=1&isAllowed=y

Gabinete do Secretário-Geral do Sistema de Segurança Interna. (2025). Relatório Anual de Segurança Interna – Ano 2024. https://www.portugal.gov.pt/pt/gc24/comunicacao/documento?i=relatorio-anual-de-seguranca-interna-rasi-2024

Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep Learning. *MIT Press*. https://doi.org/10.1007/s10710-017-9314-z

Hand, D. J. (2006). Classifier Technology and the Illusion of Progress. *Statistical Science*. https://doi.org/10.1214/088342306000000060 https://diariodarepublica.pt/dr/detalhe/lei/51-2023-220949538

Johnson, S., Bernasco, W., Bowers, K., Elffers, H., Ratcliffe, J., Rengert, G., & Townsley, M. (2007). Space-Time Patterns of Risk: A Cross National Assessment of Residential

Burglary Victimization. *Journal of Quantitative Criminology*, 23. https://doi.org/10.1007/s10940-007-9025-3

Kitchin, R. (2014). Big Data, New Epistemologies and Paradigm Shift. *Big Data & Society*, 1, 1–12. https://doi.org/10.1177/2053951714528481

Le Monde. (2024). How algorithmic video surveillance was used during the Paris Olympics. https://www.lemonde.fr/en/france/article/2024/08/16/how-algorithmic-video-surveillance-was-used-during-the-paris-olympics_6716745_7.html

Le Monde. (2025). Le Conseil constitutionnel censure la prolongation de la vidéosurveillance algorithmique. https://www.lemonde.fr/pixels/article/2025/04/24/le-conseil-constitutionnel-censure-la-prolongation-de-la-videosurveillance-algorithmique_6599713_4408996.html

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

Lei n.º 51/2023, de 28 de agosto. Define os objetivos, prioridades e orientações da política criminal para o biénio de 2023-2025, em cumprimento da Lei n.º 17/2006, de 23 de maio, que aprova a Lei Quadro da Política Criminal. *Diário da República n.º 166/2023: I Série de 28 de agosto.*

Lum, K., & Isaac, W. (2016). To Predict and Serve?. *Significance*, *13*, 14–19. https://doi.org/10.1111/j.1740-9713.2016.00960.x

Mali, B., Bronkhorst-Giesen, C., & Den Hengst, M. (2017). Predictive Policing – Lessen voor de toekomst. *Politieacademie*. https://www.websitevoordepolitie.nl/predictive-policing-in-nederland-en-duitsland/

Mohler, G., Short, M., Malinowski, S., Johnson, M., Tita, G., Bertozzi, A., & Brantingham, P. (2015). Randomized Controlled Field Trials of Predictive Policing. *Journal of the American Statistical Association*, 110, 00–00. https://doi.org/10.1080/01621459.2015.1077710

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

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

Oosterloo, S. K., & Schie, G. V. (2018). The Politics and Biases of the "Crime Anticipation System" of the Dutch Police. https://ceur-ws.org/Vol-2103/paper_6.pdf

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, Instituto Superior de Ciências Policiais e Segurança Interna]. Repositório Comum. http://hdl.handle.net/10400.26/35180

Pérez Lagos, C., & Ghassemi, M. (2025). Discours sur les risques autour de la vidéosurveillance algorithmique: La couverture médiatique des JOP 2024. *Études de communication*, *64*, 91–112. https://doi.org/10.4000/14b5j

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). Predictive policing: The role of crime forecasting. RAND Corporation. https://www.rand.org/pubs/research_reports/RR233.html

Ratcliffe, J. (2016). *Intelligence-Led Policing*.

Regulamento (UE) n.º 679/2016 do Parlamento Europeu e do Conselho - Regulamento Geral sobre a Proteção de Dados (RGPD). (2016*). Jornal Oficial da União Europeia*, L 119, 1–88. https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679

Regulamento (UE) n.º 1689/2024 Regulamento da Inteligência Artificial. (2024). *Jornal Oficial da União Europeia*, L 272, 1–95. http://data.europa.eu/eli/reg/2024/1689/oj

Reuters. (2024). Olympics - How France plans to use AI to keep Paris 2024 safe. https://www.reuters.com/sports/olympics-how-france-plans-use-ai-keep-paris-2024-safe-2024-03-08/

Ribeiro, M., Singh, S., & Guestrin, C. (2016). *«Why Should I Trust You?»: Explaining the Predictions of Any Classifier* (p. 1144). https://doi.org/10.1145/2939672.2939778

Russell, S., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach, Global Edition*. Pearson Education. https://books.google.pt/books?id=cb0qEAAAQBAJ

Schuilenburg, M., & Soudijn, M. (2023). Big data policing: The use of big data and algorithms by the Netherlands Police. *Policing: A Journal of Policy and Practice*, *17*. https://doi.org/10.1093/police/paad061

Security Magazine (2021). Uma nova Era para a analítica de vídeo. 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. 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. https://revistasegurancaeletronica.com.br/o-que-e-video-analitico-e-como-ele-funciona/

Szeliski, R. (2022). Computer vision (2nd ed.). *Springer Nature Switzerland AG 2022*. https://doi.org/10.1007/978-3-030-34372-9

Tilley, N. (2009). *Crime Prevention*. Willan. https://books.google.pt/books?id=ptQQLgAACAAJ

Townsley, M., Homel, R., & Chaseling, J. (2003). Infectious Burglaries: A Test of the Near Repeat Hypothesis. *British Journal of Criminology*, *43*. https://doi.org/10.1093/bjc/azg615

Willems, D., & Doeleman, W. (2014). Predictive policing. Wens of werkelijkheid. *Het Tijdschrift voor de Politie*. https://event.cwi.nl/mtw2014/media/files/Willems,%20Dick%20-%20CAS%20Crime%20anticipation%20system%20_%20predicting%20policing%20in%20Amsterdam.pdf

Willems, D. (2017). *Predicting criminal events with data science*. Data Science Utrecht Meet Up, Utrecht - Países Baixos.

Zatsepina, L., & Ludvigsen, J. (2025). Algorithmic Olympics: Exploring the ethical and social implications of AI surveillance through the case of Paris 2024. *International Journal of Sport Policy and Politics*, *17*, 1–22. https://doi.org/10.1080/19406940.2025.2529201