



INSTITUTO SUPERIOR DE CIÊNCIAS POLICIAIS E SEGURANÇA INTERNA
VI CURSO DE COMANDO E DIREÇÃO POLICIAL

Trabalho Individual Final

**A inteligência artificial e o policiamento preditivo: riscos,
benefícios e desafios à atividade policial**

Auditor

Rui Pedro Gonçalves Dias

Lisboa, 03 de outubro de 2025

Resumo

O presente estudo centrou-se na análise da utilização de sistemas de inteligência artificial no policiamento preditivo. Através da análise massiva de dados históricos relativos a um determinado padrão criminal, torna-se possível a delimitação de áreas geográficas de alto risco, onde um fenómeno criminal é mais provável de ocorrer, permitindo uma melhor alocação de recursos policiais. Contudo, vários dilemas éticos relacionados com a utilização destes sistemas, tornam a sua implementação desafiante. Para além da falta de transparência dos algoritmos, destaca-se, o risco de enviesamento de dados, que poderá condicionar a classificação de uma zona como alto risco, contribuindo para uma sensação discriminatória e de violação de privacidade por parte da população.

Da análise de experiências internacionais de países como Holanda, Itália, França e Alemanha, verificou-se um benefício cauteloso. Perante a necessidade de regulamentação e definição de limites éticos, a União Europeia criou o Regulamento de Inteligência Artificial, que salienta a necessidade de supervisão humana e classificação do risco destes algoritmos. Assim, a utilização da inteligência artificial no policiamento preditivo poderá contribuir como inovação tecnológica nas forças de segurança, através da sua utilização como ferramenta de análise de dados altamente regulada, transparente e auditada, usada como mecanismo de suporte à atividade policial.

Palavras-chave: Inteligência artificial, policiamento preditivo, União Europeia; Regulamento de inteligência artificial,

Abstract

This study focused on analysing the use of artificial intelligence systems in predictive policing. Through the large-scale analysis of historical data related to a specific criminal pattern, it becomes possible to delineate high-risk geographical areas where a criminal phenomenon is more likely to occur, allowing for a more effective allocation of police resources. However, several ethical dilemmas related to the use of these systems make their implementation challenging. In addition to the lack of transparency in the algorithms, the risk of data bias may influence the classification of an area as high risk, contributing to a sense of discrimination and violation of the population's privacy.

From the analysis of international experiences in countries such as the Netherlands, Italy, France and Germany, a cautious benefit was observed. Faced with the need for regulation and the definition of ethical boundaries, the European Union created the Artificial Intelligence Act, which highlights the importance of human supervision and risk classification of these algorithms.

Thus, the use of artificial intelligence in predictive policing may contribute as a technological innovation for security forces, through its application as a highly regulated, transparent and audited data analysis tool, used as a support mechanism for police activity.

Keywords: Artificial intelligence, predictive policing, European Union, AI Act

Índice

Resumo	ii
Abstract.....	iii
Introdução.....	1
Estado de Arte	2
Contextualização teórica.....	2
O Policiamento Preditivo	2
IA no policiamento preditivo	4
Dilemas éticos associados ao uso da IA no policiamento preditivo	5
Método	7
Perspetivas.....	8
O policiamento preditivo na UE	8
Holanda	8
Itália.....	9
França.....	10
Alemanha	10
Regulamentação europeia e nacional.....	12
Discussão e conclusão	16
Referências	20

Introdução

A inteligência artificial (IA) apresenta uma ubiquidade crescente na sociedade contemporânea, marcando presença em múltiplos sistemas do quotidiano e assumindo-se como uma prioridade nas agendas políticas de governos e organizações internacionais, incluindo a União Europeia (UE) (Fernandes, 2020).

A aplicação da IA no domínio da segurança pública tem despertado um interesse significativo por parte das polícias, que vislumbram nesta tecnologia uma oportunidade para otimizar a sua eficácia e eficiência perante orçamentos e recursos humanos limitados (EUCPN, 2022; EUROPOL, 2024).

É neste contexto que emerge o policiamento preditivo, que pode ser entendido como a aplicação de técnicas de recolha e análise de dados provenientes de diversas fontes, que são posteriormente utilizados pelas polícias, órgãos de investigação criminal e outras entidades competentes, com o objetivo de antecipar padrões de comportamento, identificar potenciais ameaças e adotar estratégias que permitam prevenir e combater a criminalidade de modo mais eficiente, contribuindo assim para a mitigação dos riscos associados à prática de futuros crimes (Silva, 2022).

A promessa de otimizar a alocação de recursos, muitas vezes escassos, e de aumentar a eficácia na prevenção criminal das organizações policiais, posiciona a IA como uma ferramenta de inovação tecnológica de enorme potencial (Fernandes, 2020; EUROPOL, 2024).

No entanto, este potencial é indissociável de desafios éticos, sociais e legais significativos, criando uma tensão fundamental em torno da sua aplicação. Se por um lado, esta tecnologia tem o potencial de transformar a aplicação da lei, ao permitir que a polícia antecipe e previna o crime, em vez de simplesmente reagir a ele (Pearsall, 2010), por outro lado, a sua eficácia é influenciada pela qualidade dos dados (Lum & Isaac, 2016; Richardson et al., 2019). Se esses dados refletirem preconceitos e desigualdades sociais existentes, a IA irá aprender e perpetuar esses mesmos preconceitos, levando potencialmente a uma vigilância desproporcional e a um policiamento excessivo de comunidades já marginalizadas, aprofundando a desconfiança no sistema (Raji, I. & Sholademi, D., 2024).

A Agência dos Direitos Fundamentais da União Europeia (2022) alerta para o facto dos algoritmos poderem levar ao policiamento desproporcional de áreas habitadas maioritariamente por minorias étnicas, infringido múltiplos direitos humanos consagrados na Carta dos Direitos Fundamentais da UE.

Em resposta a estes desafios, a UE publicou recentemente o Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024 (*AI Act*), que entrou em vigor em agosto de 2024 (Parlamento Europeu & Conselho da União Europeia, 2024).

Neste contexto, importa refletir sobre os riscos, benefícios e desafios da utilização da IA no policiamento preditivo, especialmente numa realidade europeia e nacional marcada por um quadro normativo em evolução.

Desta forma, com este estudo pretendeu-se responder à seguinte pergunta de partida: Poderá a IA, aplicada ao policiamento preditivo, constituir-se como uma inovação tecnológica relevante para a atividade policial?

Numa fase inicial deste estudo será efetuada uma contextualização teórica sobre o conceito de policiamento preditivo, o papel da IA associada ao mesmo e os dilemas éticos inerentes à sua utilização. Em seguida, optou-se por analisar experiências internacionais de implementação do policiamento preditivo em Estados-Membros da UE, como a Holanda, Itália, França e Alemanha. Por fim, procedeu-se à análise do quadro normativo europeu e nacional relativo a este tema, com destaque para o *AI Act*.

Com o intuito de dar resposta à pergunta de partida e respetivas perguntas derivadas do presente estudo, foi efetuada uma reflexão que sintetiza os benefícios e os riscos, mas também as perspetivas futuras para uma utilização responsável e eficaz desta tecnologia no policiamento preditivo.

Estado de Arte

Contextualização teórica

O Policiamento Preditivo

O conceito de policiamento preditivo tem evoluído ao longo dos tempos, no entanto, de acordo com Meijer e Wessels (2019), não existe uma definição completamente consensual. Uma das primeiras definições formais surge em 2010 com Pearsall (Mugari & Obioha, 2021). Segundo este autor o policiamento preditivo poderia ser definido como a obtenção de dados de uma determinada fonte e sua análise no sentido de antecipar, prevenir e responder mais eficazmente a futuros crimes (Pearsall, 2010).

Uma definição amplamente referida na literatura é a de Perry et al (2013) onde o policiamento preditivo é definido como aplicação de técnicas de análise quantitativa para

identificar alvos prováveis para a intervenção policial, com o objetivo de prevenir crimes ou resolver crimes já ocorridos através de previsões estatísticas.

Por sua vez Uchida (2009), utiliza uma definição mais relacionada com o uso de tecnologia, referindo que a capacidade de predição de crimes tem por base a análise computadorizada da informação acerca de crimes previamente cometidos.

De acordo com Perry et al. (2013), o policiamento preditivo pode subdividir-se em duas partes fundamentais: a formulação de uma predição e a geração consequente de algum tipo de intervenção ou investigação policial no sentido de diminuição do crime. O processo de predição compreende etapas fundamentais: recolha e análise de dados acerca de crimes que possam produzir predições; intervenção policial que atue sobre o crime em análise (ou que ajude a resolver crimes passados). De acordo com o mesmo autor, o tipo de intervenção policial está de acordo com o crime em causa, podendo ser mais genérica, específica para o crime em causa ou intervenção específica para um determinado problema. Torna-se assim essencial uma avaliação constante da mesma, de forma a verificar os resultados pretendidos, permitindo voltar ao início do ciclo, alterando o tipo de intervenção policial efetuada, se necessário (Perry et al., 2013).

Neste modelo de policiamento preditivo, os métodos preditivos podem dividir-se em quatro categorias de acordo com Perry et al (2013), nomeadamente:

- a) método para predição de crimes (identificam locais e tempos de maior probabilidade de ocorrência de crimes);
- b) método para predição de agressores (identificam pessoas em risco para cometer crimes no futuro);
- c) método de predição vítimas de crimes (identificam pessoas ou grupos com probabilidade de serem vítimas de crimes);
- d) método de predição de identidade de perpetradores de crimes (criam perfis que tentam correlacionar potenciais criminosos com crimes passados).

O modelo baseado na predição de crimes baseado na sua localização (*place-based*), tem sido estudado amplamente nos últimos anos, inserindo-se no âmbito da criminologia ambiental (McDaniel & Pease, 2021). Neste âmbito a análise criminal centra-se no local de ocorrência do crime, partindo do princípio de que este e o ambiente oferecem a oportunidade para a prática de determinado delito, recolhendo dados, padrões criminais e influências ambientais com o objetivo de prevenir esse tipo de crime naquela localização específica. (Jeffrey, 1971 citado por McDaniel & Pease, 2021). A identificação destas localizações

permite uma tentativa de modificações que permitam a redução criminal. A criação de mapas específicos de zonas de risco (*hot spots*), ajudam na identificação de locais de maior probabilidade de ocorrência de determinados tipos de crime, facilitando a adoção de estratégias para a sua prevenção (Perry et al., 2013; McDaniel & Pease, 2021).

O modelo de avaliação de risco no terreno (*Risk Terrain Model*) de Caplan e Kennedy (2011), defende a avaliação do risco com base em camadas separadas de mapas representativas da influência espaço temporal e intensidade de um fator de risco criminal, criando num sistema de informação geográfica, as quais são combinadas de forma a formarem um mapa final de risco de terreno. De acordo com este modelo, a alocação de forças policiais nestas áreas poderá tornar o combate ao crime mais efetivo (Ferguson, 2017).

IA no policiamento preditivo

A informação acerca de dados criminais passados e ocorrência criminais centra-se em grandes bases de dados das forças de segurança. O *Big Data* representa a informação reunida em grandes bases de dados, a qual pode ser analisada e demonstrar correlações inesperadas (Zarsky, 2011). Extrair e analisar dados dessa dimensão torna-se um processo lento e complexo.

De acordo com Saisse (2017) a análise de dados pode ser classificada em quatro categorias: preditiva, a qual considera a prospeção de dados históricos no sentido de analisar probabilidades; prescritiva, analisa estudos de casos e avalia possíveis consequências sobre ações tomadas; análise diagnóstica, na qual são tomadas decisões baseadas em factos ocorridos; descritiva, avalia os dados de uma forma em tempo real fornecendo respostas mais imediatas.

Atendendo à elevada dimensão de dados a serem analisados, surgem ferramentas de IA, as quais agilizam a extração de dados criminais, eventos e correlação ambiental, permitindo uma identificação de padrões criminais a determinados locais e alocação de recursos mais efetiva (EUROPOL, 2024). A tecnologia utilizada para análise destes dados, utiliza algoritmos específicos, os quais não são mais do que processos matemáticos que realizam extrapolações e previsões de acordo com as correlações dos dados (EUCPN, 2022).

Machine learning é uma área da IA relacionada com o desenvolvimento de programas de *software* com a capacidade de aprender a executar uma tarefa, tendo como base sua própria experiência (EUCPN, 2022). Algoritmos de *machine learning* têm sido utilizados no policiamento preditivo para analisar dados criminais e tentar prever padrões futuros (Kim et al, 2018).

Correlações entre determinados tipos de crime e fatores geográfico-ambientais podem também ser estabelecidas, situação que facilita a adoção de estratégias de prevenção criminal (Elluri et al, 2019). A componente preditiva do policiamento, pode ser otimizada recorrendo a estes algoritmos, uma vez que é efetuada uma análise detalhada de dados criminais relativos a áreas geográficas, permitindo delimitar *hot spots* criminais específicos e direcionar os recursos policiais para esses locais (Mandalapu et al, 2023).

Já o *deep learnig*, como o caso das redes neuronais, é o termo que se refere ao *machine learning* usando múltiplas camadas de elementos computadorizados e é dependente de *hardware* sofisticado (Russell e Norvig, 2022). O algoritmo permite a análise dos dados criminais com relação tempo-espacial, permitindo estabelecer padrões de crime em determinados locais, e a construção de um modelo preditivo que identificará locais futuros desse tipo de incidente (Hossain et al., 2020; Saraiva et al., 2022). Estes algoritmos assumem também relevância na análise de videovigilância, utilização de drones para monitorização de atividade criminal (Shah et al., 2021) e permitem uma análise rápida e automatizada de dados criminais de várias fontes. Desta forma, potenciam a rápida resposta ao crime (Saraiva et al., 2022).

Assim, a utilização da IA aliada ao policiamento preditivo poderá contribuir para uma alocação mais otimizada de recursos humanos, e mais direcionada para áreas consideradas críticas para determinados fenómenos criminais, bem como para a organização de patrulhamento em datas e locais específicos (EUROPOL 2024; Perry et al., 2013; Ratcliffe, 2016). Além disso permite, ainda, o estabelecimento de novas práticas operacionais, nomeadamente criação de protocolos de combate a crime, em que os elementos são devidamente treinados na análise e interpretação de dados e adoção de uma resposta criminal adaptada (Hoffman, 2019).

Dilemas éticos associados ao uso da IA no policiamento preditivo

Se por um lado a utilização de IA associada a estratégias de policiamento preditivo, parece tornar mais efetivo o trabalho policial no que concerne à alocação e gestão de recursos, questões éticas de transparência, privacidade e viés têm sido levantadas (Raji & Sholademi, 2024).

Em relação à transparência, a utilização de IA é definida como criando um efeito de opacidade (Castelvecchi, 2016). Ou seja, os algoritmos de IA são bastante complexos mesmo para interpretação humana, e retiram as conclusões da forma como foram programados, muitas vezes já com algum nível de opacidade como forma de proteção de dados induzida

pelo fabricante (Burrell, 2016). A forma como os algoritmos analisam os dados e retiram determinada conclusão é, assim, opaca e pouco transparente. Estes algoritmos produzem resultados, sem expor a forma como lá chegaram ou a sua lógica (Burrell, 2016).

Também o facto de os algoritmos serem desenvolvidos por indivíduos e organizações diferentes, levanta também a questão de ser difícil a responsabilização no caso de violações de direitos humanos, resultante da utilização de sistemas de IA no policiamento preditivo (Thompson, 1980).

A qualidade da análise de dados depende diretamente da qualidade e da forma como os dados são inseridos, podendo enviesar os resultados obtidos (Yeung, K., 2019). O enviesamento dos dados analisados numa determinada área geográfica, por contributos históricos acerca de técnicas de policiamento prévias que podem ter recebido várias influências socioculturais, pode condicionar os resultados e classificar essa área sempre como sendo de elevado risco criminal, classificando determinadas comunidades e bairros sempre como de alto risco (Lum, 2017). Esta situação poderá originar um sistema de *feedback loop*, em que de forma repetida as forças policiais são deslocadas para essas áreas, situação que reforçará ainda mais o enviesamento (Veal et al., 2023). A própria forma como os dados são recolhidos de forma massiva através de bases de dados, muitas vezes enviesados por práticas antigas, pode perpetuar esse enviesamento e conduzir a práticas discriminatórias sobre determinados grupos (Ferguson, 2017).

Além disso, o equilíbrio entre a necessidade de garantir a segurança dos cidadãos e o respeito à sua privacidade, deve ser bem balanceado, pois, muitas vezes, os dados são obtidos através de dados criminais históricos, comunicação social e mecanismos que possuem informação pessoal não consentida pelos cidadãos (Raji & Sholademi, 2024).

A utilização de IA no policiamento preditivo levanta também algumas questões acerca da liberdade e confiança dos cidadãos (Raji & Sholademi, 2024). Ao basear-se na colheita de dados e antecipação criminal de determinadas comunidades, pode conduzir a uma situação de marginalização e suspeição exacerbada sobre determinados grupos (Brayne, 2017), criando nos indivíduos um sentimento de violação de privacidade e direitos fundamentais. Além disso, a confiança nas forças policiais poderá ser abalada se as comunidades se sentirem estigmatizadas ou demasiado monitorizadas, criando um efeito oposto ao pretendido (Lum & Isaac, 2016).

Neste sentido, torna-se de crucial importância a criação de regulamentação própria relativa à utilização da IA, que vise salvaguardar os limites éticos e legais da sua utilização, nomeadamente no policiamento preditivo.

Método

A metodologia de uma investigação compreende "o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo de produzir conhecimentos válidos e verdadeiros" (Lakatos & Marconi, 2017, p.96).

No presente estudo, optou-se por uma abordagem qualitativa, centrada na análise de literatura científica, relatórios institucionais, páginas institucionais eletrônicas e legislação relativa à aplicação da IA no policiamento preditivo.

Esta opção metodológica e a formulação do problema de investigação resultam de um processo de revisão da literatura, motivado pela crescente relevância que a IA tem vindo a assumir na sociedade e na segurança em particular, partindo da necessidade de compreender o fenómeno a partir de múltiplas perspetivas teóricas e normativas.

O ponto de partida de um projeto de investigação deve consistir na formulação de uma pergunta central, um exercício através do qual o investigador se esforça por traduzir, da forma mais exata e focada possível, a essência daquilo que procura saber, elucidar ou compreender melhor (Quivy & Van Campenhoudt, 1998). Neste estudo, a pergunta de partida já enunciada e que orienta toda a investigação é a seguinte: Poderá a IA, aplicada ao policiamento preditivo, constituir-se como uma inovação tecnológica relevante para a atividade policial?

De forma a dar resposta à pergunta inicial do presente estudo, foram elaboradas as seguintes perguntas derivadas:

1. Qual o paradigma da implementação ao nível da UE dos modelos de policiamento preditivo com recurso a IA?
2. Que limites e salvaguardas o quadro normativo europeu e nacional tem vindo a estabelecer para regular o uso dos sistemas de IA aplicados ao policiamento preditivo?

Perspetivas

O policiamento preditivo na UE

Holanda

A utilização de estratégias de policiamento preditivo tem assumido grande interesse nos últimos anos, nomeadamente na Europa e, embora esteja descrita a sua utilização em vários países, a Holanda foi o primeiro país a implementar um sistema de policiamento preditivo em grande escala e a nível nacional (EUCPN, 2022; Strikwerda, 2021). O sistema denomina-se *Crime Anticipation System* (CAS) e foi implementado em 2013, após ter sido desenvolvido pela Unidade Regional de Polícia de Amsterdão e estendeu-se inicialmente a 160 unidades de polícia em todo o país (Schuilenburg & Soudijn, 2023). O funcionamento deste sistema consiste na elaboração de um mapa geográfico abrangendo uma área de 125x125m, onde o sistema faz as suas predições acerca do risco de determinados tipos de crimes ocorrerem (Meijer et al., 2021). O risco é codificado num sistema de cores: vermelho para risco elevado, laranja para risco médio e amarelo para risco reduzido, sinalizando, assim, os chamados *hot spots* (Galič et al., 2022). A informação é baseada nos dados das últimas duas semanas e atualizada diariamente pelas forças policiais (Galič et al., 2022).

Numa fase inicial, o sistema incidia sobretudo em crimes como furtos em residências, roubos na via pública e outros roubos, tendo sido alargado mais tarde para furtos por carteirista, furtos em empresas, furto no interior de veículos e furto de bicicletas (Willems, 2014). A polícia de Amsterdão utiliza equipas policiais denominadas *flex teams*, as quais são deslocadas para estas áreas de maior risco e para cada equipa, dois analistas fornecem orientações com base nas predições realizadas pelo sistema CAS (Hardyns & Rummens, 2018).

Durante o período de outubro 2013 a julho 2014, o sistema foi capaz de prever corretamente 15% dos furtos no interior de residências e 33% dos assaltos (De Grawn, 2014). Uma das principais justificações para a utilização deste sistema seria que o preconceito humano e enviesamento seria removido e substituindo por análises de dados supostamente objetivas e neutras, tornando o policiamento mais eficiente e justo (Mutsaers & Nuenen, 2023). Contudo, o sistema cria um ciclo de viés de confirmação, onde os preconceitos existentes na sociedade e na polícia são inseridos no sistema, que por sua vez gera dados que parecem confirmar esses mesmos preconceitos (Mutsaers & Nuenen, 2023). Assim, o sistema não é capaz de se limitar a interpretar de forma passiva o espaço urbano em causa (Jefferson, 2017).

Para além do risco de enviesamento descrito, de acordo com De Vries e Smit (2016), o sistema poderá também afetar a privacidade individual e ter impacto na vida pessoal dos habitantes das áreas definidas como alto risco pelo sistema, contribuindo para a sensação discriminatória. Os mesmos autores destacam, ainda, o risco de perda da capacidade individual técnica da polícia e do seu julgamento com base na experiência e intuição dos profissionais.

Itália

Em Itália existem vários sistemas de IA utilizados no âmbito do policiamento preditivo, dos quais se destaca o sistema x-law, desenvolvido pela Inspetora da polícia Lombardo (Gialuz & Quattrocchio, 2023). Este sistema de IA baseado no *deep learning*, pretende prevenir a ocorrência determinados tipos de crimes, tais como roubos e furto por carteirista em locais previamente identificados como de risco, de forma a permitir a utilização mais efetiva de recursos policiais (XLAW, 2022).

Desde 2013, o sistema tem sido implementado em várias cidades italianas, tais como Nápoles, Veneza, Salerno, Modena e Parma (XLAW, 2022). Os objetivos da utilização deste sistema de IA no policiamento preditivo nestas cidades foram: aumento da eficiência operacional; poupanças em termos de gestão de custos na segurança da comunidade, através de redução de número de patrulhamentos, gastos com combustíveis e desgaste emocional das equipas; impacto motivacional nas equipas policiais; aumento da perceção de segurança por parte dos cidadãos e da reputação das forças de segurança (XLAW, 2022).

Os resultados da aplicação desta tecnologia mostraram uma redução criminal em todas as cidades, nomeadamente: cerca de 43% em Parma, 38% em Salerno, 34% em Prato, 22% em Nápoles, 19% em Veneza e 16% em Modena (XLAW, 2022). Impactos importantes na redução de custos para as forças policiais, também se verificaram em todas as cidades onde o sistema foi implementado (XLAW, 2022).

Assim, este método preditivo policial com base na IA, foi mais eficaz na redução da criminalidade face ao método tradicional de aquisição de dados estatísticos de dados passados, evitando o desperdício de recursos humanos e financeiros (XLAW, 2022). Além disso a diminuição da criminalidade nas áreas analisadas, não se refletiu num deslocamento dos mesmos crimes para áreas próximas (XLAW, 2022).

França

Em 2017, onze territórios da área de intervenção policial da *Gendarmerie* (polícia militar Francesa) em França adotaram o sistema de policiamento preditivo *PAVED* (Godé, 2020). O sistema de IA cria *hotspots* espaço-temporais baseados na análise estatística de dados passados, focando-se, sobretudo, em crimes como furtos a residências, a estabelecimentos comerciais e roubos a viaturas, sendo os dados atualizados mensalmente (Godé, 2020). O sistema fornece possibilidades de visualização, nomeadamente: gráficos de *hotspots* que identificam a laranja as zonas de alto risco e a verde as zonas de baixo risco; funções de aumento de imagem dessas áreas de forma a obter-se uma visualização mais detalhada do local e dos arruamentos ou uma visão mais alargada (Godé, 2020).

De acordo com Lecorps e Tissandier (2022), utilizando um modelo de estimativa estatística, a utilização do sistema permitiria uma redução de cerca de 5% nos roubos de carros, ou seja, uma redução de cerca de 100 carros roubados por departamento onde a tecnologia foi aplicada. Além disso não se verificou impacto nos roubos domicílio, nem na criminalidade em áreas circundantes (Lecorps e Tissandier, 2022).

Este sistema foi colocado em pausa desde 2019, tendo sido apontado como pouco transparente acerca da natureza das variáveis sociodemográficas inseridas no algoritmo, bem como da sua natureza de causa-efeito (La Quadrature du Net, 2025). Além disso, foi descrito como discriminatório, uma vez que as variáveis inseridas têm em conta, predominantemente populações específicas mais direcionadas para a imigração e precariedade, o que acaba por conduzir a um policiamento excessivo em áreas/bairros específicos (La Quadrature du Net, 2025).

Alemanha

Na Alemanha, dentro dos vários *softwares* de policiamento preditivo baseado em locais, destaca-se o *Pre Crime Observation System* (PreCobs), o qual tem sido utilização para predizer a probabilidade de ocorrência de furtos em residências (Egbert & Krasmann, 2019). Este sistema está em utilização desde 2015 pelo departamento policial da Baviera (Knobloch, 2018). O sistema cria locais, designados áreas observacionais, onde o crime tem maior probabilidade de ocorrer de acordo com dados prévios e análise retrógrada, criando, assim, as predições no formato de alertas, os quais são visualizados em quadrados de cerca de 250x250m de dimensões (Seidensticker & Bode, 2018).

Outros sistemas como KimPro, muito utilizado em Berlim, funcionam de forma semelhante e também baseados em modelos de predição de locais de ocorrência de furtos em interior de residências (Sekensticker et al., 2018).

Por sua vez, os sistemas KLB-operativ e PreMap, também focados no furto no interior de residências, pretendem otimizar o trabalho das forças de segurança, fornecendo-lhe os locais de predição de crimes, que podem ser visualizados em *smartphones* e aplicações pelos agentes da polícia, com visualização das áreas problemáticas, os *hotspots* (Sekensticker et al., 2018).

De acordo com Sekensticker et al. (2018), o projeto SKALA, foi implementado no sentido de avaliar os modelos de policiamento preditivo, baseados sobretudo em furtos no interior residências e comerciais. O sistema pretendia avaliar a eficiência das intervenções policiais baseadas no modelo de policiamento preditivo, bem como as potencialidades e limitações das mesmas e teve início em fevereiro de 2015, e uma duração de quase três anos, durante os quais a metodologia da polícia preditiva foi extensivamente testada (Sekensticker et al., 2018; Seidensticker & Schwarz, 2022).

Segundo Bode (2018), o projeto estabeleceu como prioridade a avaliação da metodologia de polícia preditiva de forma independente e com um sistema aberto, garantindo transparência e rastreabilidade, bem como soberania sobre os dados, o que implicava que nenhuma informação policial seria processada por fornecedores de serviços externos, permitindo que fosse utilizada pelos próprios polícias. O projeto também avaliou a probabilidade de ocorrência de outros crimes, baseada em hipóteses, que incluíam não apenas dados policiais, mas também socioeconômicos e demográficos (Bode, 2018; Seidensticker & Bode, 2018). Demonstrou com sucesso a viabilidade da metodologia de polícia preditiva para complementar o combate ao crime de roubos a residências, tendo sido, na altura, considerado um sucesso, passando a ser implementado nos 16 principais departamentos de investigação criminal da polícia (Seidensticker & Bode, 2018).

Em fevereiro de 2023, o Tribunal Constitucional Federal alemão declarou inconstitucionais as leis dos estados de Hesse e Hamburgo que permitiam a análise automatizada de dados pela polícia para a prevenção de crimes (Brady, 2023). O tribunal considerou que a criação de perfis de pessoas com potencial para cometer crimes antes de estes acontecerem representava uma violação do direito geral da personalidade e do direito à autodeterminação informativa, consagrados na Lei Fundamental alemã (Brady, 2023).

Regulamentação europeia e nacional

Com a crescente utilização da IA em vários domínios na UE, surgiu a necessidade de criação de regulamentação adequada, no sentido de equilibrar os avanços tecnológicos com garantias éticas e de preservação dos direitos fundamentais.

Em 2018, surgiu o reconhecimento da importância da IA pela Carta Europeia de Ética sobre o Uso da IA em Sistemas Judiciais e seu ambiente, admitindo o uso por parte das polícias de algoritmos para identificar locais de ocorrência de crimes (Alves, 2023).

Ao mesmo tempo, a UE, criou um grupo de peritos de alto nível, que elaboraram um relatório com diretrizes éticas para uma IA confiável (Pedroso & Santos, 2024). Estes requisitos incluem: a necessidade de ação e supervisão humanas; a garantia de solidez técnica e segurança; privacidade através de uma administração de dados adequada; transparência nas decisões tomadas; diversidade, a não discriminação e a equidade; contribuir para o bem-estar social e ambiental; assegurar a devida responsabilização pelos seus resultados (Grupo de Peritos de Alto Nível Sobre a Inteligência Artificial, 2019).

Segundo Pedroso e Santos (2024), estes requisitos quiseram garantir que a conceção, programação e aplicação da IA, devem estar sob supervisão humana e obedecer a padrões éticos universalmente reconhecidos, tendo sempre como prioridade o respeito e a segurança dos seres humanos (Pedroso & Santos, 2024).

Em 2020, foi criado o Livro Branco sobre a IA (Comissão Europeia, 2020), que aponta diretrizes, propostas de políticas, estratégias ou recomendações sobre o desenvolvimento, uso e regulação da IA. Este documento propõe uma estratégia para que a Europa desenvolva e implemente a IA de uma forma que impulse a sua competitividade e inovação, ao mesmo tempo que garanta que a tecnologia seja fiável, segura e alinhada com os valores e direitos europeus (Comissão Europeia, 2020).

Em 2021, iniciou-se a Proposta de Regulamento do Parlamento Europeu e do Conselho que instituiu regras harmonizadas para a IA e classificou as tecnologias de policiamento preditivo como sistemas de IA de risco elevado (Alves, 2023).

O processo foi concluído em março de 2024 com a aprovação do *AI Act* pelo Parlamento Europeu, tornando-se a primeira legislação global, aplicável a todas as pessoas e entidades públicas ou privadas que produzam ou utilizem sistemas de IA, em todos os Estados-Membros da UE (Pedroso & Santos, 2024).

Com a aprovação do *AI Act*, a UE pretendeu introduzir uma abordagem baseada no risco, promovendo a utilização de IA centrada no ser humano e nos direitos fundamentais

(Barros, 2024). A sua criação pretendeu ainda garantir a inovação associada à utilização da IA, mas salvaguardando um elevado nível de proteção nas questões de saúde, segurança e direitos humanos na UE, respeitando a democracia e a lei (Comissão Europeia, 2025).

Segundo a Comissão Europeia (2025), o *AI Act* descreve uma abordagem baseada no risco que classifica os sistemas de IA em quatro categorias distintas:

- i. Risco inaceitável: sistemas de IA que são proibidos;
- ii. Risco elevado: sistemas de IA que representam uma ameaça considerável para a saúde, segurança ou direitos fundamentais e que estão sujeitos a exigências e obrigações legais estritas;
- iii. Risco em matéria de transparência: sistemas sujeitos a obrigações de transparência;
- iv. Risco mínimo a nulo: sistemas de IA que não são regulamentados;

De acordo com o *AI Act*, o uso de sistemas de IA para policiamento preditivo individual é proibido, nos termos do artigo 5, n. 1 alínea d), uma vez que não se pode colocar no mercado, disponibilizar ou usar IA para avaliar ou prever o risco de alguém cometer um crime quando essa avaliação é feita apenas com base em perfis, traços de personalidade ou características pessoais (Díaz González, 2025).

Esta proibição não estava na proposta original, tendo sido uma das inovações significativas incorporadas durante o processo legislativo, em parte devido às observações críticas do Comité Europeu para a Proteção de Dados e da Autoridade Europeia para a Proteção de Dados (Díaz González, 2025).

De acordo com a Comissão Europeia (2025), para que a utilização de um sistema de IA seja proibido, é necessário que se verifiquem, cumulativamente, as três condições seguintes:

- a) o sistema de IA tem de ser introduzido no mercado, em serviço ou simplesmente utilizado;
- b) o sistema de IA deve prever ou avaliar o risco de um indivíduo cometer um crime;
- c) a previsão ou a avaliação de risco deve assentar pelo menos umas das seguintes condições:
 - i. a criação de um perfil de um indivíduo;
 - ii. a avaliação da personalidade de um indivíduo com base nas suas características.

Estas práticas, de natureza particularmente danosa e abusiva, são alvo de proibição uma vez que representam uma afronta aos valores consagrados pela UE, nomeadamente a dignidade humana, a liberdade, a igualdade, a democracia e o Estado de direito, bem como aos direitos fundamentais, como o direito à não discriminação, à proteção de dados pessoais e à privacidade e à proteção dos direitos da criança (Parlamento Europeu & Conselho da União Europeia, 2024).

Excluem-se desta proibição os sistemas de IA que funcionem como ferramenta de apoio à análise humana sobre o envolvimento de um indivíduo em atividades criminosas, quando tal análise já assenta em dados factuais, objetivos e verificáveis (Comissão Europeia, 2025).

Os sistemas de IA de policiamento preditivo que não se enquadram na proibição, são considerados de risco elevado e estão sujeitos a um conjunto rigoroso de regras e requisitos estabelecidos no anexo III, do *AI Act*. (Díaz González, 2025).

Destaca-se ainda que, o regulamento não se aplica em sistemas elaborados exclusivamente para fins militares, de defesa ou segurança nacional (Comissão Europeia, 2025). O artigo 2.º do *AI Act*, prevê uma série de exclusões gerais do âmbito que são relevantes para uma compreensão completa da aplicação prática das proibições listadas no artigo 5.º do *AI Act*, nomeadamente a utilização de sistemas de IA no âmbito da segurança nacional, defesa e fins militares (Parlamento Europeu & Conselho da União Europeia, 2024).

De acordo com o Tribunal de Justiça da União Europeia (2020), o termo ‘segurança nacional’ refere-se ao:

ao interesse primordial de proteger as funções essenciais do Estado e os interesses fundamentais da sociedade e inclui a prevenção e a repressão de atividades suscetíveis de desestabilizar gravemente as estruturas constitucionais, políticas, económicas ou sociais fundamentais de um país, em especial de ameaçar diretamente a sociedade, a população ou o Estado enquanto tal, como, nomeadamente, as atividades terroristas (p.43).

Será da responsabilidade de cada Estado-Membro definir os seus principais interesses de segurança e adotar as medidas apropriadas para garantir a sua segurança interna e externa (Tribunal de Justiça da União Europeia, 2020).

Foram estabelecidos prazos para entrada em vigor da aplicação do *AI Act*, destacando-se as seguintes datas: 2 de fevereiro de 2025, inicia-se a aplicação dos capítulos

das disposições gerais e práticas proibidas; 2 de agosto de 2026, a aplicação para sistemas de risco elevado (com algumas exceções); 2 de agosto de 2027, a aplicação da obrigação técnica remanescente para os sistemas de risco elevado (Parlamento Europeu & Conselho da União Europeia, 2024).

Atualmente, Portugal já deu cumprimento à obrigação estabelecida pelo artigo 77.º do *AI Act*, que determina que cada Estado-Membro publique, até 2 de novembro de 2024, uma lista das autoridades responsáveis por supervisionar a legislação europeia que protege os direitos fundamentais (Digital.gov.pt, 2025). No caso português, destacamos a Inspeção-Geral da Administração Interna como entidade competente na área da Administração Interna (Digital.gov.pt, 2025).

Ao nível do quadro normativo nacional, encontramos a Lei n.º 59/2019, de 8 de agosto (transpõe a Diretiva (UE) 2016/680), que estabelece regras para o tratamento de dados pelas autoridades competentes em matéria criminal. Daqui resulta que a legislação proíbe as decisões suscetíveis de afetar significativamente os cidadãos, sejam tomadas exclusivamente com base em processamento automatizado de dados, incluindo a definição de perfis (Lei n.º 59/2019, de 8 de agosto, art. 11º). Na mesma linha, a Lei n.º 27/2021, de 17 de maio, também conhecida como a Carta Portuguesa de Direitos Humanos na Era Digital, estabelece princípios para uso de novas tecnologias. O seu artigo 9.º, dedicado à IA, exige que a utilização de sistemas de IA pelas entidades públicas ou privadas respeite os direitos fundamentais e observe princípios de explicabilidade, transparência, segurança e responsabilização, prevenindo preconceitos e todas as formas de discriminação.

No que respeita à posição Comissão Nacional de Proteção de Dados (CNPD), embora não exista um parecer específico sobre policiamento preditivo, as orientações assumidas em matérias relacionadas, como a videovigilância com recurso a IA, demonstram uma forte preocupação com a proteção de dados pessoais, a discriminação e o respeito pela privacidade dos cidadãos, assumindo a classificação da utilização de IA pelas forças de segurança como de risco elevado à luz do *AI Act*. (Comissão Nacional de Proteção de Dados, 2024). É, portanto, previsível que a CNPD adote uma posição cautelosa quanto à implementação de sistemas de IA no policiamento preditivo, exigindo uma base legal sólida, uma avaliação rigorosa e a demonstração da sua necessidade e proporcionalidade.

Em 2023, o governo aprovou a Resolução do Conselho de Ministros n.º 91/2023, relativa à Estratégia Integrada de Segurança Urbana (EISU), visando reforçar a segurança dos cidadãos (Presidência do Conselho de Ministros, 2023). A EISU, menciona explicitamente, o envolvimento da Polícia de Segurança Pública e Guarda Nacional

Republicana, no desenvolvimento de “análise de dados de apoio ao policiamento preditivo; identificação de hotspots, padrões e tendências criminais” (Presidência do Conselho de Ministros, 2023, p.41). Neste documento, já se antevê a vontade política em potenciar a análise inteligente de dados nas forças de segurança.

Discussão e conclusão

A análise teórica demonstrou que o policiamento preditivo, potenciado pela IA, materializa a capacidade de analisar vastos conjuntos de dados para identificar *hotspots* e padrões criminais, como definido por Perry et al. (2013) no seu conceito de policiamento preditivo, permitindo uma gestão de recursos teoricamente mais inteligente e eficaz. Também a Comissão Europeia (2025), considera que os sistemas de IA usados para prever a criminalidade, através da análise de dados históricos para detetar padrões e calcular a probabilidade de um novo crime acontecer, oferecem às autoridades policiais a oportunidade de aumentar a sua eficiência e adotar uma postura proativa na prevenção do crime, otimizando a alocação de recursos, muitas vezes escassos.

A utilização de sistemas de IA no policiamento preditivo baseado em locais nos países europeus analisados, mostrou ser benéfica em termos de previsão de criminalidade, como no caso da utilização do sistema CAS na Holanda (De Grawn, 2014), bem como na redução de alguns tipos de crime, como em Itália (XLAW, 2022) e França (Lecorps & Tissandier, 2022). No caso alemão verificou-se ser uma ferramenta útil como complemento ao combate à criminalidade (Seidensticker & Bode, 2018).

Contudo, de acordo com a Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais, embora o policiamento preditivo seja uma ferramenta de IA usada pela polícia para detetar padrões e correlações em conjuntos de dados, esta tecnologia é incapaz de determinar a causa desses padrões ou de prever de forma fiável o comportamento de um indivíduo (Parlamento Europeu, 2021).

Alinhamos com o Parlamento Europeu, quando afirma que não pode ser o único critério para justificar uma intervenção policial (Parlamento Europeu, 2021), mas pode, de facto, assumir-se como uma ferramenta complementar à atividade policial, que contribua quer para uma melhor gestão de recursos, quer para o combate à criminalidade, como verificado nos países analisados.

Respondendo à primeira questão derivada, sobre o paradigma de implementação na UE, verifica-se que não existe uma abordagem uniforme, mas sim uma tendência de experimentação cautelosa, cada vez mais balizada pela necessidade de um quadro legal robusto. Países como a Holanda, Itália, França e Alemanha foram pioneiros na adoção de *softwares* de policiamento preditivo, focados maioritariamente em modelos *place-based* para prevenir crimes. No caso alemão, com a decisão do Tribunal Constitucional Federal em 2023, que embora não vise diretamente a utilização de IA, estabelece-se um limite poderoso que condiciona a forma como os dados baseados em pessoas podem ser utilizados para fins preditivos, na tentativa de não constituírem uma violação do direito geral da personalidade e do direito à autodeterminação informativa, consagrados na Lei Fundamental alemã (Brady, 2023).

Em relação à segunda questão derivada, verifica-se que face às diversas questões éticas implícitas à utilização da IA em vários domínios da sociedade, nos quais podemos incluir a sua utilização pelas forças de segurança, surge a criação do *AI Act*, no sentido de garantir que a utilização da IA na UE seja segura, ética, transparente e respeite os direitos humanos fundamentais (Comissão Europeia, 2025). O *AI Act* classifica o policiamento preditivo baseado em locais como alto risco e reforça a necessidade de obedecer a regras específicas, tais como a supervisão humana. Já o artigo 5º do *AI Act*, criado posteriormente, destaca as proibições à utilização da IA, nomeadamente no policiamento preditivo baseado em indivíduos, à semelhança da proibição consagrada pelo Tribunal Constitucional alemão.

Apesar dos sistemas de IA de policiamento preditivo que baseiam as previsões dos crimes na localização, em zonas ou em locais específicos, não serem abrangidos pela proibição do artigo 5º do *AI Act*, uma vez que as previsões de crime por localização analisam as áreas e não o indivíduo (Comissão Europeia, 2025), a postura de aplicação pelos Estados Membros deverá ser cautelosa.

Destaca-se que o regulamento não se aplica a sistemas de IA utilizados exclusivamente para fins militares, de defesa ou de segurança nacional (Comissão Europeia, 2025). No entanto, apesar da existência de uma definição, a delimitação exata do que constitui segurança nacional é um ponto que requer supervisão constante no sentido de se evitarem utilizações abusivas, devendo ser definida, de forma clara, pelos Estados Membros (Tribunal de Justiça da União Europeia, 2020).

Perante a ausência de legislação nacional que regule a utilização da IA pelas forças de segurança, tal como se verifica no caso de Portugal, vislumbra-se ser relevante, de acordo com Muir e O'Connell (2025) a criação de uma Comissão de Ética para a Tecnologia

Policial, que emitiria diretrizes para as forças de segurança sobre diferentes casos analisados, bem como sobre o uso destas tecnologias. Isto proporcionaria maior clareza relativamente as regras de utilização da IA e poderia ser reforçado por mecanismos de participação e deliberação tanto pública como de peritos (Muir & O'Connell, 2025). Em França, já existe um comité de ética ligado ao Ministério das Forças Armadas francês, criado em 2019 e formado por civis e militares, que supervisiona questões éticas relacionadas com uso de novas tecnologias de defesa, em especial IA militar (Vincent, 2025). No caso do Reino Unido, também foi criado um comité de ética de dados em 2019 pelo Comissário de Polícia e Criminal de West Midlands em conjunto com a polícia local, atuando como painel consultivo independente para avaliar projetos de ciência de dados e IA da unidade de análise de dados da Polícia (West Midlands Police & Crime Commissioner, 2025).

Assim, concordamos com Latini et al. (2025) quando sugere a criação destas entidades para assegurar a supervisão da implementação da utilização da IA no policiamento preditivo. Neste sentido, de acordo com Coelho et al. (2023), a criação destes comités de ética compreende seis passos fundamentais:

- 1) *definição de responsabilidades*: definição do responsável por acompanhar o processo de criação de programa de gestão de riscos de soluções de IA na organização;
- 2) *diagnóstico de soluções*: levantamento de quais soluções, utilizam técnicas de IA, para gerar decisões automatizadas e/ou auxiliar tomada de decisão;
- 3) *relatório geral de impacto*: enumeração de quais são os riscos que podem gerar reflexos nos direitos das pessoas;
- 4) *programa de governança e gestão de riscos*: criação de um programa para à análise e acompanhamento do desenvolvimento de soluções de IA na organização;
- 5) *definição dos princípios éticos da organização para o uso da IA*: listagem de quais são os princípios éticos centrais a serem seguidos pela organização;
- 6) *criação do Comitê de Ética*: criação ou adaptação de uma estrutura para avaliação das soluções de IA usadas pela organização.

Para além da criação de comités de ética específicos, as Instituições deverão, de acordo com Macnish (2024), investir na introdução de dados de qualidade nas suas bases de dados, na tentativa de minimizar o enviesamento e garantir que refletem, de forma clara, o que se passa na comunidade. Devem, ainda, garantir a revisão humana detalhada dos dados

e resultados algorítmicos e investir na formação junto da comunidade, de forma a garantir a transparência e confiança da população, explicando como a utilização da IA irá servir o bem-estar da mesma (Macnish, 2024). Além disso, as forças de segurança devem investir no recrutamento de especialistas nesta área, nomeadamente engenheiros, analistas e cientistas de dados, devendo, igualmente, ser fomentada a interação entre as polícias e a indústria de produção das tecnologias de IA, bem como o investimento claro por parte do Estado nas forças de segurança (Muir & O'Connell, 2025).

Assim, podemos inferir que a utilização de sistemas de IA no policiamento preditivo poderá contribuir como inovação tecnológica relevante nas forças de segurança, cujo futuro passará, sobretudo, pela sua utilização como ferramenta de análise de dados altamente regulada, transparente e auditada, usada como instrumento de suporte às forças de segurança. O sucesso da sua implementação dependerá menos da potência do algoritmo e mais da robustez da moldura ética e legal que o rodeia. A inovação não estará completa até que a tecnologia possa ser implementada de forma transparente, explicável e equitativa, fortalecendo, a confiança entre a Polícia e a comunidade.

Referências

- Agência da União Europeia para os Direitos Fundamentais. (2022). *Bias in algorithms – Artificial intelligence and discrimination*.
<https://fra.europa.eu/en/publication/2022/bias-algorithm>
- Alves, C. A. (2023). O policiamento preditivo – desafios processuais e substantivos. *Anatomia do Crime*, 17, 107–133.
<https://anacrimine.scholasticahq.com/article/87665-o-policiamento-preditivo-desafios-processuais-e-substantivos>
- Barros, G. O. (2024). *Em Análise - Regulamentação da Inteligência Artificial na União Europeia: Uma análise do AI Act*. Gabinete de Estratégia e Estudos.
<https://www.gee.gov.pt/pt/documentos/estudos-e-seminarios/artigos/10243-gee-em-analise-regulamento-da-inteligencia-artificial/file>
- Brady, G. (2023). *Germany says no to predictive policing – The rule of law challenges posed by algorithms*. EmildaI. <https://emildai.eu/germany-says-no-to-predictive-policing-the-rule-of-law-challenges-posed-by-algorithms/>
- Brayne, S. (2017). Big Data Surveillance: The Case of Policing. *American Sociological Review*, 82(5), 977–1008. <https://doi.org/10.1177/0003122417725865>
- Bode, F. (2018). *Project “SKALA”: Predictive policing in North Rhine-Westphalia* [Apresentação de conferência]. Stockholm Criminology Symposium.
https://criminologysymposium.com/download/18.7f57ba351641b9cdc3dd183/1531985235780/TUE07_Felix_Bode.pdf
- Burrell, J. (2016). How the machine ‘thinks’: Understanding opacity in machine learning algorithms. *Big Data & Society*, 3(1). <https://doi.org/10.1177/2053951715622512>
- Caplan, J. M., & Kennedy, L. W. (2011). *Risk terrain modeling compendium*. Rutgers Center on Public Security.
- Castelvecchi, D. (2016). *Can we open the black box of AI?* *Nature*, 538, 20–23.
<https://doi.org/10.1038/538020a>
- Coelho, A. Z., Klafke, G., Maito, D. C., Latini, L. M. D., Maruca, G., Chow, B. G., & Feferbaum, M. (2023). *Governança da inteligência artificial em organizações: Framework para Comitês de Ética em IA – versão 1.0*. CEPI FGV Direito SP.
<https://hdl.handle.net/10438/33736>

- Comissão Europeia. (2020). *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. (2025). *Comunicação da Comissão: Orientações da Comissão sobre as práticas de inteligência artificial proibidas estabelecidas pelo Regulamento (UE) 2024/1689 (Regulamento da Inteligência Artificial)* (C(2025) 5052 final). <https://digital-strategy.ec.europa.eu/pt/library/commission-publishes-guidelines-prohibited-artificial-intelligence-ai-practices-defined-ai-act>
- Comissão Nacional de Proteção de Dados. (2024). *Parecer sobre a observância das regras relativas à segurança do tratamento de dados no pedido de autorização para a utilização de câmaras portáteis de uso individual pela Polícia Marítima* (Parecer n.º 2024/24).
- De Graauw, J. S. (2014). *Tijdruimtelijk voorspellen van criminele incidenten* [Dissertação de mestrado]. Vrije Universiteit Amsterdam. <https://vu-business-analytics.github.io/internship-office/reports/report-graauw.pdf>
- Díaz González, G. M. (2025). Prohibited artificial intelligence practices (Chapter II). In A. Huergo Lora (Ed.) & G. M. Díaz González (Coord.), *The EU regulation on Artificial Intelligence: A commentary* (pp. 37–78). Wolters Kluwer Italia.
- Digital.gov.pt. (2025). *Lista de entidades que supervisionam a proteção dos direitos fundamentais no âmbito do artigo 77.º do AI Act*. Consultado em 05 de setembro de 2025, de <https://digital.gov.pt/regulamentacao/ai-act/lista-de-entidades-que-supervisionam-a-protecao-dos-direitos-fundamentais-no-ambito-do-artigo-77-do-AI-Act>
- Egbert, S., & Krasmann, S. (2019). Predictive policing: not yet, but soon preemptive?. *Policing and Society*, 30(8), 905-919. <https://doi.org/10.1080/10439463.2019.1611821>
- Elluri, L., Mandalapu, V., & Roy, N. (2019). *Developing machine learning based predictive models for smart policing*. SMARTCOMP 2019. <https://doi.org/10.1109/SMARTCOMP.2019.00053>
- EUCPN (2022). *Artificial intelligence and predictive policing: risks and challenges*. Brussels:EUCPN. <https://eucpn.org/sites/default/files/document/files/PP%20%282%29.pdf>

- EUROPOL. (2024). *AI and policing: the benefits and challenges of artificial intelligence for law enforcement*. Publications Office of the European Union.
<https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing>
- Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.
- 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
- Galič, M., Das, A., & Schuilenburg, M. (2022). *AI and administration of justice: predictive policing and predictive justice in the Netherlands*.
<https://doi.org/10.13140/RG.2.2.17944.88320>
- Gialuz, M., & Quattrocchio, S. (2023). *AI and the administration of criminal justice in Italy*. Association Internationale de Droit Pénal (AIDP).
<https://www.penal.org/sites/default/files/files/A-01-23.pdf>
- Godé, C., Brion, S., & Bohas, A. (2020). The affordance-actualization process in a predictive policing context: Insights from the French military police. In *Proceedings of the 28th European Conference on Information Systems (ECIS)*.
https://aisel.aisnet.org/ecis2020_rp/167
- Grupo de peritos de alto nível sobre a inteligência artificial. (2019). *Orientações éticas para uma IA de confiança*. Comissão Europeia.
<https://digital-strategy.ec.europa.eu/pt/library/ethics-guidelines-trustworthy-ai>
- Hardyns, W., & Rummens, A. (2018). Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. *European Journal of Criminal Policy and Research*, 24, 201-218. <https://doi.org/10.1007/s10610-017-9361-2>
- Hoffman, A. (2019). The Future of Policing: Training Officers in Data-Driven Practices. *Police Chief*, 86(1), 44-49.
- Hossain, S., Abtahee, A., Kashem, I., Hoque, M. M., & Sarker, I. H. (2020). Crime prediction using spatio-temporal data. In N. Chaubey, S. Parikh, & K. Amin (Eds.), *Communications in Computer and Information Science: Vol. 1235. Computing Science, Communication and Security* (pp. 277–289). Springer.
https://doi.org/10.1007/978-981-15-6648-6_22

- Jefferson, B. J. (2017). Digitize and punish: Computerized crime mapping and racialized carceral power in Chicago. *Environment and Planning D: Society and Space*, 35(5). <https://doi.org/10.1177/0263775817697703>
- Kim, S., Joshi, P., Kalsi, P. S., & Taheri, P. (2018). *Crime analysis through machine learning*. In *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)* (pp. 415–420). IEEE. <https://doi.org/10.1109/IEMCON.2018.8614828>
- Knobloch, T. (2018). *Vor die Lage kommen: Predictive Policing in Deutschland. Chancen und Gefahren datenanalytischer Prognosetechnik und Empfehlungen für den Einsatz in der Polizeiarbeit*. Stiftung Neue Verantwortung; Bertelsmann Stiftung. <https://www.interface-eu.org/archive/publications/2337>
- Lakatos, E. M., & Marconi, M. de A. (2017). *Fundamentos de metodologia científica* (8.^a ed.). Atlas.
- La Quadrature du Net. (2025). 'Predictive' policing in France: Against opacity and discrimination, why a ban is needed. <https://www.laquadrature.net/wp-content/uploads/sites/8/2025/05/polpred050525.pdf>
- Latini, L. M. D., Klafke, G. F., & Feferbaum, M. (2025). *Comitês de ética em inteligência artificial (IA): por onde começar?* GV-executivo, 24(1). <https://doi.org/10.12660/gvexec.v24n1.2025.92932>
- Lecorps, Y., & Tissandier, G. (2022). *PAVED With Good Intentions? An Evaluation of a French Predictive Policing System*. SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.4314831>
- Lei n.º 27/2021, de 17 de maio, Carta Portuguesa de Direitos Humanos na Era Digital, Diário da República n.º 95/2021, Série I de 2021-05-17. <https://diariodarepublica.pt/dr/detalhe/lei/27-2021-163442504>
- 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>
- Lum, K. (2017). *Limitations of mitigating judicial bias with machine learning*. *Nature Human Behaviour*, 1, artigo 0141. <https://doi.org/10.1038/s41562-017-0141>
- Lum, K., & Isaac, W. (2016). To predict and serve? *Significance*, 13(5), 14–19. <https://doi.org/10.1111/j.1740-9713.2016.00960>

- Macnish, K. (2024). *Policing, AI and Digital Ethics*. Sopra Steria. Consultado em 10 de setembro de 2025, de <https://www.soprasteria.co.uk/insights/blogs/details/policing-ai-and-digital-ethics>
- Mandalapu, V., Elluri, L., Vyas, P., & Roy, N. (2023). *Crime Prediction Using Machine Learning and Deep Learning: A Systematic Review and Future Directions*. arXiv. <https://doi.org/10.48550/arXiv.2303.16310>
- McDaniel, J. L. M., & Pease, K. G. (2021). *Predictive Policing and Artificial Intelligence* (1ª ed.). Routledge. <https://doi.org/10.4324/9780429265365>
- Meijer, A., Lorenz, L., & Wessels, M. (2021). Algorithmization of bureaucratic organizations: Using a practice lens to study how context shapes predictive policing systems. *Public Administration Review*, 81(1). <https://doi.org/10.1111/puar.13391>
- Meijer, A., & Martijn, W. (2019). Predictive policing: Review of benefits and drawbacks. *International Journal of Public Administration*, 42, 1031–1039. <https://doi.org/10.1080/01900692.2019.1575664>
- Mugari, I., & Obioha, E. E. (2021). Predictive Policing and Crime Control in The United States of America and Europe: Trends in a Decade of Research and the Future of Predictive Policing. *Social Sciences*, 10(6), 234. <https://doi.org/10.3390/socsci10060234>
- Muir, R., & O'Connell, F. (2025). *Policing and artificial intelligence*. The Police Foundation. <https://www.police-foundation.org.uk/publication/policing-and-artificial-intelligence/>
- Mutsaers, P., & van Nuenen, T. (2023). Predictively policed: The Dutch CAS case and its forerunners. In J. Beek, T. Bierschenk, & A. Kolloch (Eds.), *Policing race, ethnicity and culture: Ethnographic perspectives from Europe* (pp. 72–94). Manchester University Press. <https://hdl.handle.net/2066/289967>
- Parlamento Europeu. (2021). *Resolução do Parlamento Europeu sobre a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciais em casos penais (2020/2016(INI))* (P9 TA(2021)0405). https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html
- Parlamento Europeu & Conselho da União Europeia. (2024). *Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho, de 13 de junho de 2024, que cria regras harmonizadas em matéria de inteligência artificial e que altera os Regulamentos (CE) n.º 300/2008, (UE) n.º 167/2013, (UE) n.º 168/2013, (UE) 2018/858, (UE)*

- 2018/1139 e (UE) 2019/2144 e as Diretivas 2014/90/UE, (UE) 2016/797 e (UE) 2020/1828 (Regulamento da Inteligência Artificial). *Jornal Oficial da União Europeia*, Série L, 12 de julho de 2024. <https://data.europa.eu/eli/reg/2024/1689/oj>
- Pearsall, B. (2010). Predictive policing: The future of law enforcement? *National Institute of Justice Journal*, 266, 16–19.
<https://api.semanticscholar.org/CorpusID:202333859>
- Pedroso, J., & Santos, A. (2024). Inteligência artificial e justiça criminal: Riscos e desafios. *Sociologia Online*, (35).
<https://doi.org/10.30553/sociologiaonline.2024.35.6>
- Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., & Hollywood, J. S. (2013). *Predictive policing: The role of crime forecasting in law enforcement operations*. RAND Corporation. <https://doi.org/10.7249/RR233>
- Presidência do Conselho de Ministros. (2023). Resolução do Conselho de Ministros n.º 91/2023, de 9 de agosto. *Diário da República*, 1.ª série, n.º 154, 124–167.
<https://diariodarepublica.pt/dr/detalhe/resolucao-conselho-ministros/91-2023-217649592>
- Quivy, R., & Campenhoudt, L. (1998). *Manual de Investigação em Ciências Sociais*. (2ª ed). Gradiva.
- Richardson, R., Schultz, J. M., & Crawford, K. (2019). Dirty data, bad predictions: How civil rights violations impact police data, predictive policing systems, and justice. *New York University Law Review*, 94(1), 192–233.
- Russell, S. J., & Norvig, P. (2022). *Artificial intelligence: A modern approach* (4th ed.). Pearson.
- Raji, I., & Sholademi, D. (2024). Predictive Policing: The Role of AI in Crime Prevention. *International Journal of Computer Applications Technology and Research*, 13(10), 66–78. <https://doi.org/10.7753/ijcatr1310.1006>
- Ratcliffe, J. H. (2016). *Intelligence-led policing* (2ª ed.). Routledge.
- Saisse, R. (2017). Big Data Contra o Crime: Efeito Minority Report. *Direito & TI*, 1(8), 16.
<https://doi.org/10.63451/ti.v1i8.79>
- Saraiva, M., Matijošaitienė, I., Mishra, S., & Amante, A. (2022). Crime prediction and monitoring in Porto, Portugal, using machine learning, spatial and text analytics. *ISPRS International Journal of Geo-Information*, 11(7), 400.
<https://doi.org/10.3390/ijgi11070400>

- Schulenberg, 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, 1–9. <https://doi.org/10.1093/police/paad061>
- Seidensticker, K., & Bode, F. S. (2018). Projekt SKALA - Predictive Policing in Nordrhein-Westfalen. *Kriminalistik*, 8-9, 537–540.
https://www.researchgate.net/publication/332170302_Projekt_SKALA_-_Predictive_Policing_in_Nordrhein-Westfalen
- Seidensticker, K., Bode, F., & Stoffel, F. (2018). *Predictive policing in Germany*. *European Journal of Law and Technology*, 9(3), 1–14. <http://nbn-resolving.de/urn:nbn:de:bsz:352-2-14sbvox1ik0z06>
- Seidensticker, K., & Schwarz, K. (2022). Using Forecasting Methods on Crime Data: The SKALA Approach of the State Office for Criminal Investigation of North Rhine-Westphalia. *Engineering Proceedings*, 18(1), 39.
<https://doi.org/10.3390/engproc2022018039>
- Shah, N., Bhagat, N., & Shah, M. (2021). Crime forecasting: A machine learning and computer vision approach to crime prediction and prevention. *Visual Computing for Industry, Biomedicine, and Art*, 4(9). <https://doi.org/10.1186/s42492-021-00075-z>
- Silva, M. T. (2022). *Policamento preditivo e direitos fundamentais*. *Expresso*. Consultado em 17 de agosto de 2025, de <https://expresso.pt/opiniao/2022-12-30-Policamento-preditivo-e-direitos-fundamentais-46fce25a>
- Strikwerda, L. (2021). Predictive policing: The risks associated with risk assessment. *The Police Journal: Theory, Practice and Principles*, 94(3), 422–436.
<https://doi.org/10.1177/0032258X20947749>
- Thompson, D. F. (1980). Moral Responsibility of Public Officials: The Problem of Many Hands. *American Political Science Review*, 74(4), 905–916.
<https://doi.org/10.2307/1954312>
- Tribunal de Justiça da União Europeia. (2020). *Acórdão do Tribunal de Justiça de 1 de outubro de 2020, La Quadrature du Net e o., processo C-511/18 (ECLI:EU:C:2020:791)*.
<https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:62018CJ0511>
- Uchida, C. D. (2009). *A national discussion on predictive policing: Defining our terms and mapping successful implementation strategies* (NCJ 230404). National Institute of Justice. <https://www.ojp.gov/pdffiles1/nij/230404.pdf>

- Veal, C., Raper, M., & Waters, P. (2023). *The perils of feedback loops in machine learning: predictive policing*. Gilbert + Tobin.
<https://www.gtlaw.com.au/insights/the-perils-of-feedback-loops-in-machine-learning-predictive-policing>
- Vincent, E. (2025). *Le comité d'éthique de la défense appelle à un usage « proportionné » de l'IA à des fins militaires*. Le Monde. Consultado em 12 de setembro de 2025, de https://www.lemonde.fr/international/article/2025/02/10/le-comite-d-ethique-de-la-defense-appelle-a-un-usage-proportionne-de-l-ia-a-des-fins-militaires_6540722_3210.html
- De Vries, A., & Smit, S. (2016). *Predictive policing: Politiewerk aan de hand van voorspellingen*. *Justitiële verkenningen*, 42(juli), 9–22. Boom | Juridisch.
<https://resolver.tno.nl/uuid:6f2bdd20-1c5d-488a-8d89-574085c96af6>
- West Midlands Police and Crime Commissioner. (2025). *Ethics panel*. Consultado em 10 de setembro de 2025, de <https://www.westmidlands-pcc.gov.uk/governance/ethics-panel/>
- Willems, D. (2014) CAS: *CAS: Crime Anticipation System — Predictive Policing in Amsterdam* [PDF].
https://event.cwi.nl/mtw2014/media/files/Willems,%20Dick%20-%20CAS%20Crime%20anticipation%20system%20_%20predicting%20policing%20in%20Amsterdam.pdf.
- XLAW. (2022). *Presentazione*. XLAW. Consultado em 19 de julho de 2025, de <https://www.xlaw.it/presentazione/>
- Yeung, K. (2019). *Responsibility and AI (DGI(2019)05)*. Council of Europe.
<https://rm.coe.int/responsability-and-ai-en/168097d9c5>
- Zarsky, T. Z. (2011). Governmental data mining and its alternatives. *Dickinson Law Review*, 116(2), 285–330.
<https://insight.dickinsonlaw.psu.edu/dlra/vol116/iss2/2/>