



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

Trabalho Individual Final

**A Inteligência Artificial no Apoio à Investigação
Criminal**

Auditor

Luís Pedro de Sá Maia

Lisboa, 3 de outubro de 2025

Resumo

A Inteligência Artificial está a moldar o mundo contemporâneo. Como processo evolutivo, tem provocado profundas transformações nas dinâmicas sociais e no funcionamento das instituições. Contudo, trata-se ainda de uma tecnologia emergente, pelo que importa avaliar se a sua utilização apresenta ganhos que justifiquem uma aposta séria nesta temática.

A Investigação Criminal rege-se por normas jurídicas rigorosas e métodos científicos comprovados, tendo como objetivo primordial a descoberta da verdade material. Neste âmbito, privilegia-se a adoção de processos que assegurem uma eficácia e eficiência máxima.

Neste estudo procede-se a uma análise aos processos de adaptação da Inteligência Artificial à Investigação Criminal, explorando os conceitos estruturantes desta tecnologia, alicerçados ao funcionamento da sua tomada de decisão, bem como os conceitos estruturantes da Investigação Criminal e do ordenamento jurídico que lhe está associado.

O ensaio promove, assim, a reflexão crítica sobre as vantagens da Inteligência Artificial para o trabalho de Investigação Criminal, bem como sobre os limites inerentes e os riscos que acarreta. Este procura ainda, identificar caminhos que permitam alcançar um equilíbrio adequado na sua aplicação.

Palavras-chave: Big Data, Ciências Forenses, Inteligência Artificial, Investigação Criminal.

Abstract

Artificial Intelligence is shaping the contemporary world. As an evolutionary process, it has brought about profound transformations in social dynamics and the functioning of institutions. However, it is still an emerging technology, so it is important to evaluate whether its use offers benefits that justify serious investment in this field.

Criminal Investigation is governed by rigorous legal standards and proven scientific methods, with the primary objective of discovering the material truth. In this context, priority is given to the adoption of processes that ensure maximum effectiveness and efficiency.

This study analyzes the processes of adapting Artificial Intelligence to Criminal Investigation, exploring the structuring concepts of this technology, grounded in the functioning of its decision-making, as well as the structuring concepts of Criminal Investigation and the associated legal system.

The essay thus promotes critical reflection on the advantages of Artificial Intelligence for Criminal Investigation work, as well as the inherent limits and risks it entails. It also seeks to identify ways to achieve an appropriate balance in its application.

Keywords: Artificial Intelligence, Big Data, Criminal Investigation, Forensic Science.

Índice

Resumo	i
Abstract.....	ii
Introdução	1
Estado da Arte	2
Contextualização Histórica.....	2
Inteligência Artificial – o conceito	4
Inteligência Artificial na Investigação Criminal	7
Metodologia.....	9
Perspetivas/Diretrizes	9
A IA nas Ciências Forenses.....	9
A IA na Gestão do Local do Crime	10
A IA na Medicina Legal	10
A IA na Lofoscopia	11
A IA no Reconhecimento Facial / Biometria	12
A IA na investigação através do <i>Big data</i>	13
A IA aplicada à Investigação Criminal em Portugal	15
A IA como meio de prova	16
A IA e os Direitos Fundamentais	18
Conclusão	19
Bibliografia	21

Introdução

Vivemos a chamada 4.º revolução industrial, caracterizada por transformações estruturais e profundas nas sociedades, decorrentes dos avanços tecnológicos. Tais processos revelam-se crescentemente complexos, na medida em que resultam da articulação e interseção de múltiplos domínios científicos e tecnológicos (Fidalgo, 2022). Nesse cenário a Inteligência Artificial (IA), configura-se como uma tecnologia de carácter transversal, integrando e potencializando diversos saberes e inovações.

O uso das ferramentas de IA são uma constante na sociedade de hoje, sendo utilizadas em várias esferas, desde as compras online, à condução e à domótica, oferecendo benefícios enormes à sociedade (Proença, 2023). Não será então admissível que, a justiça criminal e a Investigação Criminal (IC) em particular, ignorem a massificação, os novos métodos e as ferramentas que esta tecnologia emergente pode trazer.

A pertinência deste estudo prende-se em primeiro lugar com a hodiernidade do tema IA. É um assunto extremamente atual e discutido amplamente pela sociedade, estando a IA em pleno processo de aceitação e adaptação.

Noutro sentido, verificamos que cada área do saber tem de se adaptar de forma particular à IA, sendo necessário analisarmos de que forma as Polícias o podem fazer, concretamente no âmbito da área deste estudo, a IC. Salientamos o facto de a IA e a IC serem duas áreas de trabalho assentes em várias ciências, contribuindo assim, para um estudo completo e abrangente.

Com a evolução da IA, surgem vários debates sobre o âmbito da sua utilização, mas como afirma Santos (2023), dúvidas não existem sobre o facto de a IA ser já uma realidade na IC, estando com certeza a ser utilizada.

Contudo, deparamo-nos com o problema da incerteza da sua real capacidade de cumprir o seu propósito em relação à IC, podendo não passar de uma tecnológica com pouca aplicabilidade operacional e de fraco apoio às atividades investigatórias, ou então, ser uma ferramenta essencial a esta mesma atividade. Há assim a necessidade de estudar o real valor da IA para a IC.

Na prossecução de se efetuar uma análise completa e esquematizada desta problemática, foram delineados os seguintes objetivos no presente estudo: analisar a construção do processo de tomada de decisão da máquina; avaliar o potencial da aplicação da IA na IC; analisar os campos em que a IA pode intervir no auxílio da IC; avaliar os limites

jurídicos da IA; e por fim, identificar os desafios que a IA coloca ao cumprimento dos direitos fundamentais.

Estado da Arte

Contextualização Histórica

A IA é um conceito vanguardista para a grande maioria da sociedade moderna. Apesar desta se estar a materializar nos últimos 50 anos, o pensamento sobre a automação e a possibilidade da inteligência da máquina já é discutida há mais de 400 anos.

Descartes, no *Discurso do Método* (2010), reflete pela primeira vez sobre a possibilidade de existirem máquinas inteligentes. Na quinta parte da sua obra, representa a existência de máquinas autómatas e pensantes, refletindo sobre a existência do pensamento fora da condição humana, o que para o próprio é impossível, pois o pensamento está intimamente ligado à condição humana, não sendo possível à máquina pensar, apenas imitar o pensamento humano.

Esta primeira visão da IA, apesar das limitações próprias dos conhecimentos da época, foi inovadora. Interpretada à luz de hoje, assume-se como atual, tendo obrigatoriamente de servir como uma base da discussão ética e moral no referencial da IA (Valério, 2022).

Na academia, é unânime a importância capital de Alan Turing (matemático, filósofo e biólogo, Inglês) na criação da IA. Autores como Sobreira (2025), Valério (2022), Andrade (2022) e Ribeiro (2020), atribuem a primeira experiência científica com IA ao “Teste de Turing” em 1950, que teve como finalidade verificar se a máquina poderia exibir um comportamento equivalente à inteligência humana, através de questões que humanos colocavam a outros humanos e à máquina.

Apesar da relevância das contribuições de Turing, a definição do conceito de IA não lhe é atribuída. Essa designação foi cunhada apenas em 1956 pelo professor John McCarthy, em cooperação com outros matemáticos, no contexto de uma solicitação de financiamento à Fundação Rockefeller, com vista a assegurar a sua investigação (Sobreira, 2025).

Com base neste conceito assumido por McCarthy, surge ainda na década de 50 – 1959 – o conceito de *machine learning*, criado por Arthur Samuel (engenheiro do IMT) como sendo umas das ferramentas essenciais para o desenvolvimento e sucesso da IA (Souza, 2022).

A reboque, assistimos na década de 60 do século XX ao surgimento do conceito de agentes racionais. Este era o nome dado a programas que tomavam as decisões acertadas perante os problemas que lhes eram demonstrados. De acordo com Ribeiro (2020), “Um agente racional é um agente que faz a coisa certa, ou seja, age para alcançar o melhor resultado ou, na presença de incerteza, o melhor resultado esperado.” (p.6). Estes programas foram sobretudo utilizados em jogos de estratégia e na resolução de problemas complexos de álgebra (Ribeiro, 2020).

Apesar deste rápido desenvolvimento da IA, em que vários autores profetizavam o triunfo das máquinas sobre a inteligência humana em cerca de 10 anos (Valério, 2022), assistimos nas décadas seguintes, 70/80, a um forte abrandamento do desenvolvimento desta tecnologia, devido a cortes no financiamento da sua pesquisa. Excertos fundamentados em publicações científicas do período em causa criticavam severamente a área, uma vez que não existiam ainda recursos computacionais capazes de sustentar sistemas de IA aplicáveis de forma efetiva ao contexto prático (Sobreira, 2025).

Com o surgir da internet comercial na década no 90 do século passado, houve um novo despertar na comunidade para as potencialidades da IA, tendo em conta a quantidade de informação que circulava na rede, havia a necessidade de se conseguir gerir toda aquela informação de forma automática, podendo a IA ser uma solução (Barbosa & Bezerra, 2020).

Assim, na primeira década do século XXI, observou-se uma expressiva mobilização de meios destinados ao avanço científico em IA, surgindo na segunda década, vários produtos acessíveis ao público baseados nesta tecnologia, como assistentes pessoais tecnológicos – Siri, Cortana, Alexa – programas de identificação facial, entre outros (Barbosa & Bezerra, 2020).

De acordo com Valério (2022), a IA desenvolveu-se de forma exponencial nos últimos anos, sendo hoje capaz de entregar utilidade, bem como no futuro, devido a 3 fatores tecnológicos: a velocidade de processamento, onde temos computadores cada vez mais rápidos a processar a informação; o *Big data*, que são a grande quantidade de dados resultantes de uma vida cada vez mais digital, passíveis de ser analisado; e a utilização da tecnologia da nuvem, o que permite aceder mais facilmente e com menos custo económico às infraestruturas digitais de ponta.

Inteligência Artificial – o conceito

Vários académicos se têm debruçado sobre o conceito de IA, alguns do ponto de vista puramente técnico, outros de um ponto de vista mais filosófico e também jurídico. Jonh McCarthy (2007) caracteriza a IA como “... *science and engineering of making intelligent machines, especially intelligent computer programs. It is related to the similar task of using computers to understand human intelligence, but AI does not have to confine itself to methods that are biologically observable.*” (p.2). Nesta definição apresentada pelo pioneiro do conceito de IA, podemos constatar que o grande objetivo da mesma é a inteligência, abrindo a possibilidade de explorar várias formas de cumprir esse objetivo, não se limitando à construção de inteligência pelo processo humano, mas abrindo assim as portas a processos ainda desconhecidos.

Uma outra definição de IA é avançada por Guerra et al. (2019), que nos sugere que a IA “... refere-se à capacidade de máquinas sistemas computacionais realizarem tarefas que normalmente requerem inteligência humana, como reconhecimento de padrões, tomada de decisões e aprendizado.” (p.3), demonstrando assim a amplitude e os inúmeros campos de intervenção que esta tecnologia pode ter.

Com vista a abranger todos os sistemas de IA que existem e que possam vir a existir, em 2024 o Parlamento Europeu no seu Regulamento de Inteligência Artificial (RIA), também conhecido por *AI Act*, definiu, no seu artigo (artg.) 3.º, a IA como:

...um sistema baseado em máquinas concebido para funcionar com níveis de autonomia variáveis, e que pode apresentar capacidade de adaptação após a implantação e que, para objetivos explícitos ou implícitos, e com base nos dados de entrada que recebe, infere a forma de gerar resultados, tais como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais.

Este foi um marco importante em termos jurídicos, ficando o conceito de IA devidamente balizado e não ao sabor de divergências académicas e ambíguas, onde cada investigador descrevia a aplicação do conceito, como aconteceu até então (Guedes, 2024).

Marques (2020), divide a IA em 5 paradigmas ou técnicas: o simbólico, onde a IA funciona e pensa seguindo regras e lógicas; o conexionista, ou neural, como lhe chama a maioria dos autores pelo facto de ser inspirado em redes neurais artificiais, tentando imitar o funcionamento do cérebro humano, onde cada unidade de processamento GPU equivale a um neurónio; o evolucionista, que usa como base de pensamento algoritmos assentes em cálculos da evolução genética ; o *swar*, que utiliza como base o pensamento de exame, onde

a máquina pensa numa lógica de colônia de insetos; e o *ensemble* que é uma utilização conjunta de todos os paradigmas (Marques, 2020).

Outros autores dividem também a IA quanto à sua capacidade de inteligência, surgindo pela primeira vez com Searle (1980) o conceito de IA fraca e IA forte. Estudos mais recentes têm se debruçado sobre esta distinção. Na perspectiva de Russel & Norving (2021), a IA fraca é aquela que tem uma missão muito específica atribuída, a qual a desempenha na perfeição, contudo quando disposta a outras realidades ou contextos, para o qual não foram criadas, não demonstra a capacidade de lidar com a situação e de resolver os problemas. A IA forte, é aquela que se vai adaptando à realidade e ao contexto a que está a ser submetida, moldando-se a qualquer tarefa, assenta sobre uma rede neural (emulador do pensamento humano), sendo bastante utilizada em investigações e desenvolvimentos científicos e académicos. Já a IA fraca é utilizada essencialmente em *chatbots*, filtros de e-mail ou assistentes virtuais (Russel & Norving, 2021).

Haenlein e Kaplan (2019) dão-nos uma definição, mais técnica e coincidente com a forma de como a IA está a ser utilizada atualmente, apresentando-a como “... *a system’s ability to interpret external data correctly, to learn from such data, and to use those learnings to achieve specific goals and tasks through flexible adaptation.*” (p.1), onde debitamos dados e atribuímos uma missão a estas máquinas, que têm como finalidade atingir o objetivo da forma mais eficiente e inteligente possível, aprendendo com a nova informação que vai chegando ao milésimo de segundo.

Esta definição de Haenlein e Kaplan vai de encontro a um conceito essencial na IA: o *machine learning*. É impensável a existência da IA sem o conceito de *machine learning*, sendo este a capacidade de aprendizagem que a máquina possui ao analisar dados, podendo modificar as suas respostas ou comportamentos sem a necessidade de ser previamente programada (Andrade, 2022).

Na perspectiva de Saias et al. (2018) o *machine learning* “...é uma área dedicada ao desenvolvimento de teorias computacionais e construção de sistemas de aprendizagem, onde a aprendizagem envolve a construção ou modificação automática de representações de dados/cenários/objetos em avaliação.” (p.2). Assim a máquina é capaz de construir o seu pensamento e tomar a sua decisão sem qualquer intervenção humana, possuindo a capacidade para ao longo do tempo ir alterando as suas decisões conforme vai ficando mais “inteligente” e apreendendo com novos dados com que vai sendo carregada.

A comunidade científica apresenta várias divisões e categorias do *machine learning*, sendo que a maioria dos autores é unânime em dividir o conceito em duas categorias: a aprendizagem supervisionada, e a aprendizagem não supervisionada (Saías *et al*, 2018).

Na primeira, a máquina necessita de ser previamente treinada com uma amostra devidamente rotulada e catalogada, para que o algoritmo perceba a forma de atuar. É-lhe dado um *input* e um *output*, sendo esta aprendizagem supervisionada e essencialmente empregue na resolução de problemas de classificação ou de regressão (Vicente, 2020).

Relativamente à aprendizagem não supervisionada, esta é mais utilizada quando estamos perante uma quantidade enorme de dados e de natureza muito complexa, onde não é possível atribuir o *output* esperado ao algoritmo, estando assim a máquina a identificar padrões de forma autónoma criando *clusters* (Saías *et al*, 2018).

É de todo relevante considerarmos o conceito de *deep learning* que se diferencia do até então analisado *machine learning*. Enquanto neste último a máquina se foca na aprendizagem de padrões para evoluir em vez de utilizar regras e conceitos programados manualmente, no *deep learning* a máquina aprende automaticamente, baseada em camadas de redes neurais que tentam imitar o funcionamento do cérebro humano (Saías *et al*, 2018).

Soares (2024), inclusive considera o *deep learning* como uma subcategoria do *machine learning*, revestindo uma grande importância quando estamos a considerar enormes volumes de dados ou padrões extremamente complexos. Marques (2022) reforça esta ideia afirmando que é um tipo de *machine learning* que “... configura parâmetros básicos sobre os dados e treina o computador a aprender sozinho através do reconhecimento de padrões em várias camadas de processamento.” (p.11).

Vivemos num mundo de dados, as vidas humanas estão a ficar cada vez mais dependentes das tecnológicas, as cidades estão a ficar cada vez mais tecnológicas sendo a criação de dados uma constante, resultando num volume imenso e até então nunca visto.

Nas nossas rotinas estão perfeitamente enraizados, os smartphones, o GPS, os sistemas de videovigilância, o controlo biométrico, ou seja, uma panóplia enorme de dados pessoais que estão constantemente a serem criados, armazenados e trabalhados, tendo assim cada pessoa a sua própria pegada digital.

Concordamos com Neto (2023), quando este defende que é impossível dissociar o conceito de *Big data* da IA, reforçamos ainda este pensamento com a metáfora de Valério (2022): “A revolução digital proveu-nos com uma quantidade de dados astronómica, que cresce diariamente a passos largos. Estes funcionam para os modelos inteligentes como a gasolina funcionava para o *Alfa Romeo 6C*” (par.8).

A definição de *Big data* não pode ser limitada à simples criação de grandes quantidades de dados, é mais do que isto, comportando duas vertentes: a da criação de dados numa grande escala por si só, podendo estes serem estruturados ou não estruturados; e a componente da tecnologia, que consiste num aglomerado de tecnologias que convertem estes dados em conhecimentos (Patrão, 2022).

Para entendermos este conceito alargado que é a IA, temos impreterivelmente de abordar o algoritmo, este é a base de tudo, a linha orientadora de toda a IA. Gonçalves *et al.* (2024) define-o como a “... sequência de comandos que instrui a máquina, expresso em linguagens de programação computacional, que informa um aplicativo ou software que ações tomar (...) os algoritmos organizam a informação em dados quantificáveis (...) os dados estruturados constituem a matéria-prima dos sistemas de algoritmos e, particularmente da IA.” (p.32).

Existem um sem número de algoritmos utilizáveis na computação, contudo ao que à IA mais interessa são os algoritmos de aprendizagem, aqueles que permitem a máquina aprender e tornar-se inteligente, tornando possível o *machine learning* e o *deep learning*. No funcionamento da IA, a máquina pode aprender com base em vários tipos de algoritmos: os de classificação, os de regressão, os de *clustering*, entre outros. Tudo depende da forma de como queremos programar o pensamento da máquina com o intuito de ela desempenhar a sua missão (Saias, *et al.* 2018).

Inteligência Artificial na Investigação Criminal

Considerando o artigo (art.) 1.^a da Lei de Organização de Investigação Criminal (LOIC) é definida a IC como “... o conjunto de diligências que, nos termos da lei processual penal, se destinam a averiguar a existência de um crime, determinar os seus agentes e a sua responsabilidade e descobrir e recolher provas, no âmbito do processo.”. Apesar da semelhança com a definição de inquérito presente no art. 262.º do Código de Processo Penal (CPP), diferencia-se pela sua finalidade. Enquanto a IC tem como fim a simples obtenção de prova, o inquérito tem o intento da obtenção de prova com vista à decisão de acusação (Augusto, 2024), daí a direção do inquérito ser da competência exclusiva do Ministério Público (MP), e a IC estar mais ligada às Polícias.

O estudo da adaptação da IA à função policial não é inédito, a Academia apresenta-nos estudos de aplicação da IA ao crime, ao policiamento preditivo, à análise do *Big data*, à tomada da decisão e à gestão.

Molarinho (2021) estuda a aplicação da IA à condição policial, abordando a utilização da IA na atividade operacional – onde se inclui a IC – demonstrando a sua aplicabilidade e as vantagens que poderão ser alcançadas com a utilização desta ferramenta, nomeadamente em mapeamento criminal e na capacidade e velocidade de análise de grandes dados, identificando de forma mais rápida e eficiente fenómenos criminais, assumindo assim o desenvolvimento tecnológico com um vetor importantíssimo nas estratégias das forças de segurança.

No que toca à utilização da IA para um policiamento preditivo – sendo este também de extrema importância para IC permitindo orientar os recursos ao saber onde o criminoso vai atuar – verificamos estudos nesta temática, alguns de âmbito mais generalista, outros de âmbito mais específico, como por exemplo Silva (2023) e Cascalho (2025) sobre a IA e a videovigilância.

Andrade (2023), num estudo mais generalista, demonstra como a utilização da IA permite às polícias através de, por exemplo *modus operandis*, antecipar movimentos dos criminosos, permitindo assim atuar na prevenção, ou quando esta seja exequível, permitir uma resposta mais rápida e por sua vez facilitadora da preservação do cenário do crime e aproveitar os padrões de análise preditiva como um auxílio à IC.

Outros estudos têm dirigido a sua atenção para a relação da IA com IC, nomeadamente da componente do *Big Data*, onde Neto (2023) mostra que na atualidade, onde a sociedade tem o conceito de *Big data* tão presente, só ferramentas de IA podem auxiliar o investigador na sua tarefa. Na mesma linha, Neiva (2019) aborda a importância do *Big data* e por consequência das ferramentas de IA na IC, defendendo o grande valor que as ferramentas de IA trazem à IC na análise de vários campos forenses.

Ao nível europeu destacamos o relatório *AI and Policing* da EUROPOL (2024), que analisa de forma profunda a transformação da atividade policial através da IA, mostrando todas as potencialidades desta ferramenta no auxílio à atividade policial, onde se inclui também a IC, sem deixar de parte os riscos que este novo paradigma traz para os direitos fundamentais.

Outros projetos e estudos mais futuristas estão em desenvolvimento, como o *sharing data to improve risk assessment*, ou como era originalmente chamado *homicide prediction project*, onde o Governo Britânico estuda novos algoritmos que permitirão à máquina prever futuros homicidas (Dodd, 2025). Este tipo de abordagem levanta várias questões ao nível ético, moral e de garantia de direitos fundamentais, contudo, apenas o referimos para indicar o grau de confiança e dependência que no futuro se irá depositar na máquina.

Metodologia

Este estudo teórico teve como fundamento a seguinte pergunta de partida: A Inteligência Artificial pode efetivamente contribuir para a eficácia e eficiência da Investigação Criminal?

Partindo desta pergunta, entendemos estabelecer as seguintes hipóteses:

Hipótese 1 (H1): A Inteligência Artificial permite obter resultados investigatórios mais rápidos, aumentando a celeridade dos processos;

Hipótese 2 (H2): A Inteligência Artificial permite chegar a resultados investigatórios inéditos, ampliando o alcance da investigação;

Hipótese 3 (H3): Os dados obtidos por meio de Inteligência Artificial são considerados prova válida.

O estudo assume uma natureza teórica e exploratória, fundamentando-se em revisão bibliográfica e análise documental, não existindo assim recolha de dados empíricos. Optamos por esta abordagem tendo em consideração o carácter emergente do tema, onde a reflexão teórica é primeiramente necessária à consolidação de pesquisas empíricas futuras.

Quanto ao método, utilizamos no nosso estudo o método dedutivo, onde partimos de um exercício de raciocínios, do geral para o particular, e com uma visão do global para o específico.

Neste estudo são aplicadas técnicas qualitativas, utilizando a pesquisa bibliográfica e documental, com vista a obter fontes primárias (normas jurídicas e documentos institucionais) e secundárias (a literatura científica) como base para sustentar a discussão e validação das hipóteses, empregando um método de análise funcionalista e crítico.

Perspetivas

A IA nas Ciências Forenses

A ciência forense é a espinha dorsal da IC moderna, é através dela que se baseiam linhas de investigação e se permitem concluir raciocínios investigatórios com base em evidências científicas indiscutíveis. Esta não é uma disciplina por si só, mas sim um conjunto de ciências específicas que trabalham em prol do estudo do crime e de auxílio à IC, produzindo prova pericial dentro de cada área específica, podendo ser da medicina, da

biologia, da química, da física, da lofoscopia, da documentoscopia ou da informática (Gomes, 2018).

A IA na Gestão do Local do Crime

Na grande maioria dos casos, é no local do crime que começa a investigação. Este revela-se de uma importância capital, podendo-nos revelar pormenores de tal forma pertinentes que podem ter a faculdade de resolver a investigação.

A análise do local do crime, recorrendo a laser scanning's com tecnologia LiDAR, aliado a um número massivo de fotografias, permite, recorrendo a IA, que softwares possam reconstruir o mesmo de forma totalmente pormenorizada, utilizando uma *Neural Radiance Fields* (NeRF), através da radiância dos objetos representados nas fotos, construindo um cenário 3D completamente digital (Rangelov *et al.* 2025).

Este mapeamento inteligente, abre portas a uma nova abordagem ao cenário do crime, permitindo estudá-lo com recurso à realidade virtual, à realidade aumentada e à realidade estendida, possibilitando analisar o cenário do crime de perspetivas visuais inéditas e descobrindo minúcias que de outra forma escapariam ao olho humano (Chango *et al.* 2025).

Um outro exemplo da utilidade da IA na interpretação do local do crime é o programa HemoVision, utilizado pela polícia Belga. Este programa através de algoritmos de *machine learning*, interpreta as fotos tiradas aos vestígios hemáticos classificando o tipo de vestígio que ali se encontra (Police Fédérale, 2024). Assim com uma simples fotografia, este programa revela ao investigador os padrões das manchas de sangue, para com isso se concluir se estamos perante projeções arteriais, de impacto de *cast-off* ou expirada e assim saber que tipo de acontecimentos estão na sua origem de uma forma rápida e eficiente, deixando de se esperar dias pela conclusão da análise forense.

O contributo da IA na gestão do local do crime, vai além do local do crime propriamente dito, é necessário também assegurar a cadeia de custódia da prova, através do seu rastreamento, bem como é necessário otimizar processos laboratoriais ou definir prioridades. Assim surgiram no mercado internacional vários softwares com componentes de IA relacionados com gestão forense.

A IA na Medicina Legal

A Medicina foi a primeira das disciplinas a ser utilizada no auxílio à IC, existindo relatos da sua utilização para o estudo do crime, desde o império Romano. No que respeita

ao contributo da IA para este campo científico, observamos atualmente a realização de múltiplos estudos em curso.

A IA já dá o seu contributo na estimativa do intervalo *post-mortem*, como demonstra o estudo de Bonicelli *et al.* (2022), em que através da utilização do *learning machine* no programa “ForensOMICS”, consegue-se obter uma resposta mais rápida e exata, do intervalo *post-mortem* de um esqueleto, recorrendo à análise do osso do fémur. Outros estudos como o de Al-Juhani *et al.* (2025), reconhecem a grande eficácia da IA datação do intervalo *post-mortem* através da análise de amostras do solo, contudo é ainda um projeto piloto, estando numa fase embrionário e requer uma maior avaliação.

Outro contributo que a IA poderá oferecer à medicina legal, e por sua vez à IC, é a datação de ferimentos resultantes de agressão. Aplicando o estudo de Tirado & Maurício (2020), pode-se verificar que através da utilização de redes neurais e do *deep learning*, a máquina é capaz de reconhecer com a exatidão de 95%, a datação de hematomas no corpo humano. Isto permite, por exemplo nos casos de agressão por violência doméstica, acelerar de forma significativa o processo sem se estar a aguardar perícias médico-legais que por vezes demoram dias.

Uma outra área da medicina legal que auxilia muitas vezes a IC é a toxicologia forense, também aqui estamos a assistir a um desenvolvimento assente na IA, exemplo disso é o programa NARCOSIS, que se assume como uma plataforma europeia de deteção de novas drogas com base nas mortes causadas pelas mesmas. Esta plataforma funciona através da identificação de características químicas através da IA, em vez da comparação como se faz até então (CORDIS). Isto é um enorme salto, quer na deteção, quer na rapidez da deteção de novas drogas psicoativas ilegais, uma vez que o atual método comparativo utilizado ordinariamente é muito mais demorado e tem limitações óbvias, pois é raro encontrar-se aquilo que não se procura.

A IA na Lofoscopia

A lofoscopia é das disciplinas mais antigas das ciências forenses, caracteriza-se por ser presente em todos os seres humanos e possuir em simultâneo padrões individualizados que acompanham a pessoa para o resto da sua vida (Martins *et al.*, 2024).

As técnicas tradicionais de recolha e comparação de impressões digitais são manuais e estão cientificamente validadas, contudo, apresentam constrangimento naturais de tempo, uma vez que a sua ação é vagarosa, quer na recolha quer na comparação (Martins *et al.*, 2024).

Com vista a ultrapassar esta lacuna, partiu-se para a possibilidade de utilização de sistemas digitais com recurso à IA para tornar este processo mais eficiente, existindo um conjunto de soluções recomendadas pela literatura, para que a máquina possa identificar de forma cabal as minutas dos vestígios lofoscópicos, sendo que a grande maioria dos autores aposta em utilização de redes neurais de IA (Cao & Jain, 2019; Cui *et al.*, 2020; Liu *et al.*, 2020; Gorgel & Eksi, 2021;).

Os sistemas computadorizados de análise de impressões digitais utilizado pelas Polícias, o *Automatic Fingertip Identification System* (AFIS), são uma realidade há décadas. Em Portugal, estando sob a alçada do Laboratório de Polícia Científica (Lei 67/2017, art.7.º n.º 3) nas suas versões modernas, estes softwares já utilizam a IA na análise e comparação das amostras lofoscópicas permitindo um match quase em tempo real.

Foi apresentado por Singh *et al.* (2024) um conjunto de vantagens da utilização da IA em relação à ferramenta tradicional, entre os quais: o software extrair apenas as características de interesse da minuta; o armazenamento eletrónica do vestígio; a rapidez com que a IA encontra correspondências e a capacidade de encontrar todas as correspondências em relação ao método tradicional; a possibilidade de efetuar pesquisas em milhares de amostras ao mesmo tempo, permitindo acelerar investigações; e por último, a dispensa da existência do perito.

A IA no Reconhecimento Facial / Biometria

O reconhecimento facial está amplamente difundido no dia-a-dia da população, sendo usado em inúmeras situações, como por exemplo, no desbloqueio de telemóveis, em registo de acessos, em verificações de assiduidade, entre outros.

A utilização desta tecnologia na IC assume particular vantagens, visto não depender da colaboração dos intervenientes, como teria de acontecer se estivessemos perante recolhas lofoscópicas, de ADN ou leituras de íris.

O reconhecimento facial é “... uma tecnologia capaz de identificar uma pessoa a partir de uma imagem digital ou de um vídeo”. (Orvalho, 2019, p.1). Contudo, a possibilidade de reconhecimento pode ser também comprometida pelo uso de acessórios, como óculos, bonés, ou por questões ambientais como os ângulos ou graus de iluminação (Rola, 2022).

A disseminação cada vez maior dos sistemas de videovigilância em Portugal, encerra uma oportunidade para a democratização da utilização de sistemas de reconhecimento facial de apoio à IC, com vista à identificação dos agentes do crime.

Face ao enorme volume de imagens e tempo de vídeo disponibilizado por sistemas de videovigilância, torna-se humanamente impossível para o investigador ficar horas a fio em frente a um ecrã, aguardando os momentos e pessoas de interesse para a investigação, assim entram em campo aplicações de IA.

Considerando o exemplo britânico, sendo estes pioneiros na utilização de sistemas de videovigilância, a Polícia Metropolitana de Londres utiliza dois tipos sistemas de monitorização de câmaras com IA incorporados: um sistema de *Live Facial Recognition* (LFR) e um sistema de *Retroactive Facial Recognition* (RFR), (Metropolitan Police, s.d.). O primeiro funciona através de um algoritmo que em tempo real cruza as imagens de videovigilância com as bases de dados de pessoas sobre as quais incidam mandados, ou então identifica a pessoa em tempo real, se os operadores assim o entenderem (Metropolitan Police, s.d.). O segundo é aplicado às imagens de videovigilância pós crime, identificando em primeira linha indivíduos de interesse para a investigação, com a posterior possibilidade de lhe reconstruir os passos do antes e do depois. Este software pode ser também aplicado a vídeos obtidos de outras fontes, como telemóveis, internet, canais de televisão e câmaras particulares (Metropolitan Police, s.d.).

No mercado empresarial atual, existem inúmeras aplicações de IA para corresponder à procura de softwares deste género, podendo ser aplicadas em vários espaços comerciais e recintos de eventos, sendo os mais utilizados o *clearview AI*, o *IDEMIA* e o *Cognitec, FaceFirst*.

Além do reconhecimento facial, a IA está a ser utilizada em outros campos de aplicação da biometria à IC, como a leitura da íris, a análise da marcha e tudo aquilo que sirva para identificar biometricamente uma pessoa. Contudo, optamos por não abordar em específico esses campos da biometria, por ainda se encontrarem em estudo e serem de aplicação prática bastante complexa.

A IA na investigação através do *Big data*

Ao contrário do panorama nacional, a aplicação de algoritmos de IA na análise de *Big data*, por parte de polícias de IC pelo mundo é uma realidade, estando já devidamente consolidada (Neto, 2023).

Estas aplicações utilizam ferramentas de IA para compilar um conjunto de dados em bruto, como localizações GPS, chamadas telefónicas, transações de dinheiro, acessos a bases de dados, passagens em portagens, viagens efetuadas, entre outras possibilidades infinitas,

detetando padrões, que de outra forma seriam impossíveis ou demorariam anos a detetar. Todas estas informações permitem ao investigador construir toda a rede criminosa a investigar ou então reconstruir todos os passos da vítima ou do criminoso, de acordo com a matéria em investigação (Europol, 2024).

Um exemplo de aplicação de instrumentos de IA na análise de *Big data* é o projeto VALCRI (Visual Analytics for Sense-making in Criminal Intelligence Analysis), desenvolvido pelo 7.º programa-quadro da União Europeia. Este através de Processamento de Linguagem Natural (PLN), aliado à mineração de padrões e *clusters*, tem a capacidade de explorar grandes volumes de dados com vista a identificar padrões e conexões para apoiar a investigação, reduzindo assim tempo e esforço de recursos no decorrer das investigações (Wong, 2018).

Este sistema foi aproveitado por Polícias como a de West Midlands Police, que utilizou o VALCRI para criar estatísticas utilizando como fonte de alimentação as bases de dados internas. A Polícia de Antuérpia aproveitando componentes e algoritmos do VALCRI, desenvolveu o seu próprio sistema chamado “FOCUS”, com capacidade para fazer análise criminal e correlações, quase em tempo real (*Intelligence-led Policing using VALCRI Visual Analytics Technology*, s.f.).

Outro exemplo de plataforma de análise de *Big data*, é o “Palantir Gotham”, que funciona através da integração de IA generativa (*API overview*, s.f.), com vista a analisar enormes quantidades de volume de dados no auxílio de investigações.

Utilizado pela Polícia Alemã do Estado de Hesse que lhe deu o nome de hessenDATA, tendo como objetivo principal efetuar análises e pesquisas em diversos bancos de dados (GPS; Redes Móveis, transações monetárias, propriedades), esta plataforma revelou-se uma ferramenta de fácil implementação e com resultados muito positivos, ao ponto de ser introduzida também em 2021 na Polícia da Renânia do Norte-Vestfália que lhe chamou *Datenbankübergreifende Analyse und Recherche* (DAR), e em 2022 na Polícia da Baviera, com o nome de *Verfahrensübergreifende Recherche und Analyse* – VeRA (Ulbricht & Egbert, 2024).

É ainda de referir a plataforma ShadowDragon, pelo facto de se dedicar à pesquisa e interpretação de *Big data* em fontes abertas, o chamado *Opens Source Intelligence* (OSINT), com base em redes sociais, registos públicos, blogs, notícias, bases de dados abertas, etc.

O ShadowDragon é uma plataforma que utiliza o *learning machine* para analisar as fontes abertas de forma a correlacionar informações para auxiliar em investigações ou para criar alertas de informação de interesse (Dekens, 2025).

Na sociedade atual, muita da informação passa pelas fontes abertas, sendo as redes sociais um manancial de informação. No relatório *AI and Policing* da EUROPOL (2024), somos alertados para a incapacidade das técnicas tradicionais de OSINT lidarem com o volume de informação atual.

Nos Estado Unidos reconheceram o problema mais cedo, o que levou a que vários departamentos de Polícia adquirissem o ShadowDragon para pesquisa e varrimento das mesmas, como o Departamento de Polícia do Massachusetts – EUA (Kath & Haddadin, 2021), a Polícia Estadual de Nova York (Gelardi, 2023), e o Departamento do Xerife do Condado de Polk no Iowa – EUA (Clayworth, 2024).

Muitos mais programas de análise de *Big data* com recursos de IA existem disponíveis para as investigações criminais levadas a cabo pelas Polícias, como o C3 Law Enforcement, o Sintelix, o SAS Law Enforcement, entre outros, sendo o sistema de funcionamento e objetivos idênticos, revelando-se pouco significativo desenvolver estes programas de forma particular.

A IA aplicada à Investigação Criminal em Portugal

Na elaboração deste estudo, efetuamos pesquisas em várias fontes primárias e secundárias sobre a utilização de aplicações de IA na atividade de IC por partes da Polícias, não encontrando qualquer evidência da sua utilização. Contudo, não excluímos a existência das mesmas, podendo estar a serem utilizadas para consumo interno, nomeadamente na análise de grandes volumes de dados e na análise criminal.

Podemos sim verificar que a Polícia Judiciária (PJ), fez e faz parte de vários grupos de trabalho europeus de desenvolvimento de tecnologia de IA aplicada à IC como são exemplos: o STARLiGHT, que visa aplicar a IA aos processos operacionais; o AIDA, que visa a análise de *Big data*; e o NARCOSIS que tem como objetivo detetar novas substância psicoativas (P.J., s.d.).

A Polícia de Segurança Pública (PSP), a 10 de setembro de 2025 efetuou uma consulta preliminar ao mercado para aquisição de serviços para a modernização do sistema de IC e conexos. Ao verificarmos as suas exigências técnicas, acreditamos que estará preparado para se ligar a aplicações externas de IA (PSP, s.d.).

A IA como meio de prova

Com a evolução cada vez mais rápida das tecnologias, vivemos na atualidade uma nova realidade processual penal, onde temos de nos adaptar de uma forma quase instantânea ao surgir de novos métodos tecnológicos de obtenção de prova. A hesitação passada, por parte dos tribunais, em validar prova obtida por meios tecnológicos em desenvolvimento está a desaparecer, provavelmente pela incapacidade de ignorar a digitalização cada vez maior da vida quotidiana (Fidalgo, 2022; Eberhardt, 2024).

No caso da prova obtida através de IA, Fidalgo (2022) assume a necessidade encorpar estas ferramentas nas admissibilidades, uma vez que “As ferramentas tradicionais da ciência forense digital não são suficientemente robustas para analisar uma tão grande quantidade de dados nem para estabelecer as necessárias correlações entre eles.” (Fidalgo, 2022, p.134).

Do ponto de vista de Santos (2023), a utilização da IA tanto pode servir para produzir prova como para adquirir prova. No primeiro caso, é a máquina que interpreta os dados de *input* e através de algoritmos gera a evidência, como acontece nos casos de perícias forenses, exemplo disso é uma perícia de balística, são as chamadas *machine-generated evidence*.

No segundo caso podemos recorrer a dados brutos registados por aparelhos de IA, como dados de Smartwatches, de domótica ou de assistentes virtuais, para conseguirmos depreender sequências de acontecimentos ou suprir lacunas pontuais em raciocínios investigatórios, são as chamadas *machine evidence* (Krum, 2024).

Analisando especificamente a *machine-generated evidence*, todos reconhecemos a sua importância no processo investigatório e o enorme contributo que dá na descoberta da verdade material, contudo, reconhecemos que no sistema processual penal nos deparamos com a incógnita da sua admissibilidade. Analisando o art. 125.º do Código de Processo Penal (CPP), diríamos que não existe qualquer dúvida na sua admissibilidade: “São admissíveis as provas que não forem proibidas por lei.”, pois no mesmo diploma, em nenhum momento, a IA é elencada como método proibido de prova.

Contudo, a análise tem de ser menos limitativa e mais abrangente, tendo de se efetuar uma análise comparativa com o n.º 8 do art. 32.º da Constituição da República Portuguesa (CRP) e garantir que nenhuma prova obtida pela IA tenha violado os requisitos do mesmo, bem como do art. 126.º do CPP dos métodos proibidos de prova (Krum, 2024).

Outra perspetiva sobre a utilização deste tipo de prova, é a de Fidalgo (2022), em que admite a possibilidade da admissibilidade da prova gerada por IA no ordenamento jurídico português, por força da Lei 109/2009, Lei do Cibercrime, em que a mesma fala no seu art. 11.º da aplicação dos novos meios de obtenção de prova, presentes naquele diploma, a todo

e qualquer crime em que seja necessário proceder à prova digital e não só a crimes cometidos por meio ou ambiente digital.

Uma das maiores problemáticas em relação a este tipo de prova é a formulação de um juízo adequado quanto à sua admissibilidade por parte do juiz, por culpa da pouca compreensão e da obscuridade de funcionamento do algoritmo (Eberhardt, 2024).

Ao tribunal cabe a perfeita compreensão da prova e da forma como ela é produzida, com vista a avaliar a sua admissibilidade e a fundamentação da sentença. Assim, quando estamos perante situações em que são necessários conhecimentos técnicos ou científicos, recorre-se a um perito (art. 350.º CPP). Nos casos de prova *machine-generated evidence* haverá a necessidade de recorrer a um perito, para explicar ao tribunal o caminho da máquina naquela decisão, decifrando o algoritmo utilizado pela mesma.

A resposta a esta compreensão não é na prática assim tão simples, por isso Fidalgo (2022) apresenta-nos o conceito de “...inteligência artificial de caixa negra...” (p.143), como o termo que se utiliza quando não se consegue descobrir o caminho que a máquina tomou para chegar aquela decisão.

Tal cenário pode acontecer pelo facto de a máquina ter uma capacidade de raciocínio de tal forma brilhante que a inteligência humana não consiga compreender (Fidalgo, 2022), ou então por a estarem a ocorrer viéses não identificados na máquina (Krum, 2024).

A questão viéses é central na validade e admissibilidade da prova, estes reportam-se “... à propensão de um modelo algoritmo de gerar previsões ou resultados que apresentam desvios sistemáticos em relação à verdade dos factos, ofendendo a imparcialidade e a objetividade...” (Krum, 2024, p.83). Isto pode acontecer devido a erros na fórmula do algoritmo, ou então devido a dados incorretos e/ou com falta de amostragem utilizados no treino de aprendizagem da máquina (Krum, 2024). Se não percebermos todo o funcionamento da máquina, não conseguiremos ter a certeza de que a prova não está contaminada por viéses.

Para tornar ainda mais complexa a perceção da prova *machine-generated evidence*, temos o facto de os principais desenvolvimentos destas tecnologias serem efetuados por empresas privadas, que fazem a questão de manter o funcionamento das suas aplicações em segredo, pois de outra forma, se o código do algoritmo fosse aberto, não obteriam lucro.

A IA e os Direitos Fundamentais

Analizado os circunstancialismos da IA no apoio à IC, importa agora aferir, de que forma a utilização destas tecnologias podem, ou não conflitar com Direitos Fundamentais, Liberdades e Garantias.

A IC rege-se pelas regras e no cabal cumprimento do estipulado no direito processual penal e, deste modo há uma série de garantias protegidas pela CRP e pelo CCP, como o princípio da legalidade, o princípio da jurisdicionalidade, o princípio do contraditório e o direito à privacidade.

O direito à privacidade, consagrado na conjugação dos art. 26.º, 34.º e 35.º da CRP, é aos dias de hoje, o direito fundamental constitucionalmente protegido que mais está colocado em causa, devido aos aperfeiçoamentos dos formas e meios de intromissão, destinados à prossecução da IC (Fidalgo, 2022).

A causa de conflito entre o direito da privacidade e a IA, prende-se essencialmente com a questão do reconhecimento facial e do *Big data*. No que ao reconhecimento facial diz respeito, evidenciamos que a utilização desta tecnologia ocorre, na maioria das vezes, sem o consentimento dos visados, indo conflitar essencialmente com o direito à reserva da vida privada e familiar (Santos, 2023). Quanto ao *Big data*, constatamos que esses dados são obtidos essencialmente através do registo e tratamento de dados pessoais, com a crescente utilização de *smartwatches*, telemóveis e computadores pessoais, pondo em causa a violação de correspondência – art.34.º CRP – e a utilização indevida de dados informáticos pessoais – art.35.º CRP (Eberhardt, 2024).

Como refere Fidalgo (2022), estes direitos fundamentais que constituem o direito de privacidade, podem em algumas circunstâncias serem restringidos, desde que a sua restrição seja proporcional e vá ao encontro dos interesses do processo. Contudo, a restrição dos mesmos (para não violar o valor jurídico fundamental a proteger) deverá estar subordinado ao princípio da jurisdicionalidade, ou seja, essas ações de carácter excecional têm de ser autorizadas e validadas por um juiz.

O que nunca poderá ser violado são as garantias do processo criminal – art.32.º CRP – especialmente a paridade entre a defesa e acusação. Ao consideramos a complexidade de funcionamento, o grande secretismo e a difícil compreensão dos algoritmos de *learning machine* e *deep machine*, verificamos que o direito de defesa está posto em causa, pois o arguido não está numa situação de paridade de armas com o Ministério Público, não podendo defender-se daquilo que não conhece (Fidalgo, 2022).

No intuito de se combater a violação dos direitos fundamentais por meio de utilização da IA, a União Europeia, a partir de 2018, começou a emanar documentos oficiais referentes às boas práticas de utilização da IA nos vários campos da sociedade. No entanto, só em 2024 se dá o grande passo de regulamentação de sistemas de IA através da publicação do Regulamento (EU) 2024/1689, o IA act. (Cruz, 2023).

Este documento tem como objetivo uniformizar a utilização e funcionamento da IA em todo o território da União, promovendo uma IA assente na ética e no respeito pelos direitos fundamentais assumidos pelos países membros, onde se inclui a privacidade e o direito de defesa (Nunes & Neta, 2024). Ao nível da transparência dos sistemas de IA, exige requisitos e formas de funcionamento muito claras para a correta compreensão de todos, do funcionamento da máquina, tipificando sanções aos fornecedores que não os cumprirem (Nunes & Neta, 2024).

Conclusão

A aplicação da IA às inúmeras ciências, funções e processos quotidianos é uma realidade, assumindo-se como uma tecnologia revolucionária pela sua capacidade de provocar mudanças profundas nas dinâmicas de funcionamento da sociedade e das instituições, bem como nos processos científicos.

Durante a realização deste estudo, verificamos que há um investimento expressivo das empresas do setor tecnológico na criação de aplicações baseadas em IA, tornando-a numa tecnologia com desenvolvimento relevante praticamente diário.

No que diz respeito aos processos de construção de decisão destas máquinas, constatamos que o mesmo se opera através de procedimentos de aprendizagem autónoma, em que através do algoritmo que foi desenhado, a máquina tem a capacidade de aprender por si só, tomando a decisão que se parece mais benéfica para cumprir o seu objetivo.

Este processo pode dar-se através de vários tipos de modos de funcionamento da máquina, utilizando paradigmas neurais, simbólicos e outros, conjugados com algoritmos de *learning machine* ou *deep machine*, de acordo com o objetivo e tipo de ciência que estamos a tratar.

O campo de aplicação da IA é infinito, podendo a IC ser um deles. Assim, podemos assistir à aplicação da IA nos campos da medicina legal, da lofoscopia, da análise criminal,

da fotografia, da biometria e outros, desde que com as conclusões de determinada ciência possamos descobrir a verdade material.

Apesar de todas essas potencialidades, verificamos no decorrer do estudo, que a utilização de várias tecnologias de IA pode colidir de forma grave com direitos fundamentais, direitos estes com importância consagrada ao nível da declaração universal dos direitos do Homem e da CRP.

Tendo em consideração a pergunta de partida cogitada e as hipóteses formuladas, concluímos o seguinte: relativamente à H1, verificamos que a utilização da IA permite aumentar de forma significativa a celeridade dos processos em investigação, ficando demonstrado que o recurso à IA através das ciências forenses e do *Big data*, diminui de forma considerável o tempo de execução de perícias e análise de dados.

No que à H2 diz respeito, ficou demonstrado que a capacidade e velocidade de processamento das tecnologias de IA, quando implementadas no *Big data*, são capazes de revelar padrões e informações que escapariam à mente humana. Por outro lado, constatamos também que o próprio algoritmo de aprendizagem das máquinas tem uma forma de construir o pensamento diferente da humana, podendo por diversas vezes abordar as incógnitas da investigação de um prisma completamente diferente, chegando a resultados inovadores, como eventualmente possa acontecer na revelação de evidências ignoradas, quando utilizamos a IA na gestão de um local do crime.

A H3 é de confirmação complexa, estando sujeita a uma série de condicionantes para poder ser confirmada. Assim, se na obtenção de prova por meio de IA houver o cumprimento destes requisitos: concordância prática de princípios jurídicos; salvaguardada pelos Direitos Fundamentais; subordinação aos princípios da legalidade e jurisdicionalidade; garantia da custódia da prova; e percepção clara do caminho lógico percorrido pela tecnologia, os resultados das ferramentas de IA são considerados prova válida.

A IA pode efetivamente contribuir de uma forma eficaz e eficiente na IC, carreando nos processos criminais prova de forma mais célere e inédita, permitindo uma justiça mais rápida e eficaz nos seus desígnios de servir a população.

Bibliografia

Al-Juhani, A.A., Gaber, A.M, Desoky, R.M., Binshalhoub A.A., Alzahrani, M.J., Alraythi, M.S., Showail, S., Aseeri, A.A. (2025). From microbial data to forensic insights: systematic review of machine learning models for PMI estimation. *Forensic Science, and Pathology*, 21(3). DOI: [10.1007/s12024-025-01002-x](https://doi.org/10.1007/s12024-025-01002-x)

Andrade, T.V. (2022). *O uso da Inteligências Artificial no Policiamento Preditivo*. (Dissertação de Mestrado, Escola de Direito da Universidade do Minho), Repositório UM. <https://hdl.handle.net/1822/93417>

Augusto, M.E.R.P. (2024). *A(s) Polícia(s) e a Investigação Criminal, A percepção dos investigadores criminais sobre o modelo de investigação criminal português, (Estudo de Caso no Distrito de Faro)*. (Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna). RCAAP. <http://hdl.handle.net/10400.26/58171>

BADOLATO, C.J., ARGENTINA, P.H.H., MARCHETTI FILHO, G. F. (2025). O uso de inteligência artificial como instrumento de auxílio nas investigações criminais brasileiras: uma análise dos softwares forenses e suas contribuições. *Revista de Ciências Jurídicas e Sociais da UNIPAR*, 28(1), 81-103. <https://doi.org/10.25110/rcjs.v28i1.2025-11189>

Barbosa, X.C. & Bezerra, R.F. (2021). Breve Introdução à História da Inteligências Artificial. *Jamaxi*, 4 (2), 90-97.

Bezerra, E. (2016). Introdução à Aprendizagem Profunda. In Vaninha, V., *Tópicos em gerenciamento de dados e informações* (57-86). SBBD.

Bonicelli, A., Mickleburgh, H.L., Chighine, A., Locci, E., Wescott, J., Procopio, N. (2022). The “ForensOMICS” approach to forensic post-mortem interval estimation: combining metabolomics, lipidomics and proteomics for the analysis of human bone. *BioRxiv*. <https://doi.org/10.1101/2022.09.29.510059>

Cao, K. & Jain, A.K. (2019). Automated Latent Fingerprint Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 41(4). <https://doi.org/10.1109/TPAMI.2018.281816>

Cascalho, J.P.A. (2025). *A Polícia, a Inteligência Artificial e o Direito: A Admissibilidade da Videovigilância Policial Inteligente*. (Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna). RCAAP. <http://hdl.handle.net/10400.26/58426>

Chango, X., Flor-Unda, O., Bustos-Estrella, A., Gil-Jimenez, P., Gomez-Moreno, H. (2025). Extended Reality Technologies: Transforming the Future of Crime Scene Investigation. *Technologies*, 13 (315). <https://doi.org/10.3390/technologies13080315>

Chitolina, C.L. (2023). *O espectro de Descartes assombra os engenheiros e entusiastas da "inteligência artificial"*. <https://www.anpof.org/comunicacoes/coluna-anpof/o-espectro-de-descartes-assombra-os-engenheiros-e-entusiastas-da-inteligencia-artificial>

Clayworth, J. (2024). *Polk County Sheriff launches internet surveillance*. Axios. <https://www.axios.com/local/des-moines/2024/04/17/surveillance-social-media-sheriff-polk-shadowdragon>

Cordis – EU, (s.d.). *Non-tArgeted foRensic multidisCiplinary platfOrm for inveStigatIon of drug-related fatalitieS*. <https://cordis.europa.eu/project/id/101168195>

Costa Ferreira, L. H. (2025). Inteligência artificial na gestão da investigação criminal. *Revista Do Instituto Brasileiro De Segurança Pública (RIBSP)*, 7(19), 29–66. <https://doi.org/10.36776/ribsp.v7i19.253>

Cruz, G.M.F. (2023). *A Regulamentação da Inteligência Artificial no Âmbito da União Europeia: Implicações para os Direitos Humanos*. (Dissertação de Mestrado, Universidade Lusófona do Porto). RCAAP. <http://hdl.handle.net/10437/14325>

Cui, Z., Feng, J., Zhou, J. (2021). Dense Registration and Mosaicking of Fingerprints by Training an End-to-End Network. *IEEE Transactions on Information Forensics and Security*, 16, 627-642. <https://doi.org/10.48550/arXiv.2004.05972>

Decreto de 10 de 1976, Constituição da República Portuguesa.

Decreto de Lei n.º 48/95, de 15 de março, Código Penal.

Decreto de Lei n.º 78/87, de 17 de fevereiro, Código de Processo Penal.

DeKens, N. (2025). *The Significance of AI and ML in OSINT to Human Investigators*. <https://shadowdragon.io/blog/ai-ml-and-human-intelligence-in-the-intelligence-analysis-process>

Descartes, R. (2010), Discurso do Método. Guimarães Editores.

Dodd, V. (2025). UK creating ‘murder prediction’ tool to identify people most likely to kill. *The Guardian*. <https://www.theguardian.com/uk-news/2025/apr/08/uk-creating-prediction-tool-to-identify-people-most-likely-to-kill>

Du, X., Hargreaves, C., Sheppard, J., Anda, F., Sayakkara, A., Le-Khac, N., Scanlon, V. (2020). *Exploring the State of the Art and the Future Potential of Artificial Intelligence in Digital Forensic Investigation*. ARES 2020: The 15th International Conference on Availability, Reliability and Security, Irlanda. <https://doi.org/10.1145/3407023.3407068>

Dusin, D., Ghanem, M.C., Ouazzane, K., Vassilev, V. (2024). A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation*, (48), 1-22. <https://doi.org/10.1016/j.fsidi.2023.301675>

Eberhardt, M.E.F (2024). Prova por inteligência artificial: desafios e caminhos para a admissibilidade no processo penal brasileiro e espanhol. In Valente, M.M.G., *Ciências criminais e inteligência artificial*, Almedina, 29-62.

Europol, (2024). *AI And Policing: The Benefits And Challenges Of Artificial Intelligence For Law Enforcement*. DOI: 10.2813/0321023.

Fernandes, L.F. (2020). Inteligência Artificial. *Polícia Portuguesa*, V(2), 30-35.

Fidalgo, S. (2022). A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo. In Rodrigues, A.M., *A Inteligência Artificial no Direito Penal*, Almedina, 129-156.

Freixo, Manuel. (2009). *Metodologia Científica: Fundamentos, Métodos e Técnicas*. Instituto Piaget.

Gelardi, C. (2023). *The State Police Are Watching Your Social Media*. Focus. <https://nysfocus.com/2023/01/13/state-police-social-media-surveillance-including-dataminr-shadowdragon-geofeedia>

Gomes, T.S.C. (2018). *Investigação Criminal E Ciências Forenses: Novas Competências da Polícia de Segurança Pública*. (Dissertação de Mestrado, Instituto Superior de Ciências Policiais e Segurança Interna). RCAAP. <http://hdl.handle.net/10400.26/25013>

Gonçalves, A., Torre, L., Melo, P.V., (2024). *Inteligência Artificial, Algoritmos e Media: Diálogos de Pesquisa*. LABCOM Comunicação & Artes.

Görgel, P. & Eksi A. (2021). Minutiae-based Fingerprint Identification using Gabor Wavelets and CNN Architecture. *Electrica*, 21 (3), 480-490. <https://doi.org/10.5152/electr.2021.21065>

Guedes, M.C. (2024). *Inteligência Artificial e Crime: Representações Sociais de Futuros Criminológicos*. (Dissertação de Mestrado, Instituto de Ciências Sociais da Universidade do Minho), Repositório UM. <https://hdl.handle.net/1822/96341>

Guerra, A.L.R., Silva, A.B., Melo, N.J.G., Júnior, O.S.L., Brasil, M.M., Joerke, G.A.O., Costa, W.L. (2024). Inteligência Artificial: a revolução tecnológica do século XXI. *Revista Caribeña de Ciencias Sociales*, 13(5), 1-22 <https://doi.org/10.55905/rcssv13n5-009>

Haenlein, M. & Kaplan, A. (2019). A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence. *California Management Review*, 61(4), 1-10. DOI:[10.1177/0008125619864925](https://doi.org/10.1177/0008125619864925).

Kath, R. & Haddadin, J. (2021). *ShadowDragon: Mass. Police Get New Social Media Monitoring Tool*. NBC. <https://www.nbcboston.com/investigations/shadowdragon-mass-police-get-new-social-media-monitoring-tool/2424128/>

Krum, A.R. (2024). *Admissibilidade Da Prova Gerada Por Inteligência Artificial*. (Dissertação de Mestrado, Faculdade de Direito da Universidade de Lisboa). Repositório da Universidade de Lisboa. <http://hdl.handle.net/10400.5/99011>

Lei n.º 49/2008, de 27 de Agosto, Lei de Organização da Investigação Criminal.

Lei n.º 67/2017, de 09 de agosto - IDENTIFICAÇÃO JUDICIÁRIA LOFOSCÓPICA E FOTOGRÁFICA.

Liu, Y., Zhou, B., Han, C., Guo, T., Qin, J. (2020). A novel method based on deep learning for aligned fingerprints matching. *Applied Intelligence*, 50, 397–416. <https://doi.org/10.1007/s10489-019-01530-4>

Luger, G.F. & Stubblefield, W.A. (1998). *Artificial Intelligence – Structures and Strategies for Complex Problem Solving* (3.º edição). Addison Wesley Longman, Inc.

Marques, M. L. (2020). *Inteligência Artificial: conceitos básicos*. Instituto Modal.

Martins, N., Silva, J.S., Bernardino, A. (2024). Fingerprint Recognition in Forensic Scenarios. *Sensors*, 24 (24), 1-21. <https://doi.org/10.3390/s24020664>

McCarthy, J. (2007). *WHAT IS ARTIFICIAL INTELLIGENCE?*. <https://www-formal.stanford.edu/jmc/>

Mendonça, M., Bovolenta, G.B., Rosa, B.O., Souza, L.B., Gongora, V.L., Garcia, E.I, Agonilha, H.C., Camargo, R.R., Tsuzuki, E.M., Laia, M.A.M, Silva, E.R.P., Gonçalves,

J.F.S., Godoy, W.F., Foggiano, A.A., Felizardo, K.R., Junior, F.A.S., (2023). Inteligência Artificial, Fundamentos, Conceitos, Aplicações e Tendências. In Martins, E.R., *Ciência, Tecnologia e Inovação: experiências, desafios e perspectivas* 3 (34-46). Atena Editora. <http://10.22533/at.ed.536230504>

Metropolitan Police, (s.d.). Facial Recognition Technology <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology/>

Middlesex University London (s.d.), *Intelligence-led Policing using VALCRI Visual Analytics Technology*. [Intelligence-led-Policing-using-VALCRI-Visual-Analytics-Technology.pdf](#)

Moleirinho, P.M.S.E. (2021). *Aplicação da Inteligência Artificial ao Serviço da Função Policial*. (Trabalho de Investigação Individual do Curso de Promoção a Oficial General, Instituto Universitário Militar), RCAAP. <http://hdl.handle.net/10400.26/38136>

Neiva, C.O.N. (2019). *Big Data na investigação criminal: previsão do risco, vigilância e expectativas sociais na União Europeia*. (Dissertação de Mestrado, Instituto de Ciências Sociais da Universidade do Minho). Repositório UM. <https://hdl.handle.net/1822/61235>

Neto, R.N. (2023). *O Big Data e a Investigação Criminal na PSP – O Contributo Para Uma Possível Inovação Tecnológica*. (Trabalho Individual Final do Curso de Comando e Direção Policial, Instituto Superior de Ciências Policiais e Segurança Interna). RCAAP. <http://hdl.handle.net/10400.26/46054>

Nunes, L.A.; Neta, A.H.A. (2024). MARCO REGULATÓRIO DA INTELIGÊNCIA ARTIFICIAL: ANÁLISE DO AI ACT DA UNIÃO EUROPEIA NO TOCANTE A PRIVACIDADE. *Direito UNIFACS*, n.º293, consultado em <https://revistas.unifacs.br/index.php/redu/article/view/9279>

Orvalho, V. (2019). Reconhecimento Facial. *Revista Ciência Elementar*, 7(04), 1-5. <https://doi.org/10.24927/rce2019.073>

Patrão, D.C. (2022). *Big data e propriedade intelectual: a (des)proteção das grandes bases de dados*. (Dissertação de Mestrado, Universidade Católica). Veritati – Repositório Institucional da Universidade Católica. <http://hdl.handle.net/10400.14/39021>

Pedroso, J. & Santos, A. (2024). Inteligência Artificial e Justiça Criminal. *Sociologia on line*, 35, 134-155. <https://doi.org/10.30553/sociologiaonline.2024.35.6>

Pereira, R.S. (2022). Sobre o uso de identificação biométrica (e de tecnologia de reconhecimento facial) para fins de segurança pública e de aplicação coerciva da lei: reflexões a propósito da proposta de regulamento europeu sobre a inteligência artificial. *Revista da Faculdade de Direito da Universidade de Lisboa*, (1), 839-865.

Piton, A. (2024). Inteligência artificial e reconhecimento facial: novas fronteiras penais?. In Valente, M.M.G., *Ciências criminais e inteligência artificial*, Almedina, 77-89.

Police Fédérale, (2024). *La KU Leuven et la Police Judiciaire Fédérale présentent une nouvelle méthode d'analyse morphologique des taches de sang sur les scènes de crime*. <https://www.police.be/5998/fr/actualites/la-ku-leuven-et-la-police-judiciaire-federale-presentent-une-nouvelle-methode-danalyse>

Polícia de Segurança Pública, (s.d). Consulta Preliminar de Mercado [https://www.psp.pt/PublishingImages/Lists/Consultas Preliminares/AllItems/Consulta%20Preliminar%20-%20Projeto%20MIC-SEI.pdf](https://www.psp.pt/PublishingImages/Lists/Consultas_Preliminares/AllItems/Consulta%20Preliminar%20-%20Projeto%20MIC-SEI.pdf)

Polícia Judiciária (s.d.). Projetos financiados. <https://www.policiajudiciaria.pt/projetos-financiados/#>

Proença, L. (2023). Inteligência artificial na segurança: um desafio ou uma inevitabilidade?. In Pombeiro, J. & Bello, M., *88 Vozes sobre Inteligência Artificial*, Oficina do livro, 438-456.

Rangelov, D., Waanders, S., Waanders, K., Genchev, E., Keulen, M.V., Miltchev, R. (2025). *Evaluating 3D Reconstruction: A Side-by-Side comparison of NeRF and Gaussian Splatting*

under various filming techniques. Advance online publication.
<https://doi.org/10.21203/rs.3.rs-7300179/v1>

Regulamento (UE) 2024/1689, do Parlamento Europeu e do Conselho de 13 de junho de 2024, *AI Act*.

Regulamento (UE) 2024/982, do Parlamento Europeu e do Conselho de 13 de março de 2024.

Ribeiro, T.R.S. (2020). *Flexible plan execution using temporal planning and probabilistic models*. (Dissertação de Mestrado, Faculdade de Ciências da Universidade de Lisboa). Repositório da Universidade de Lisboa. <http://hdl.handle.net/10451/47996>

Rola, E.C.S. (2022). *Os principais contributos da inteligência artificial para o processamento de imagens digitais a utilizar na segurança pública*. (Dissertação de Mestrado, Faculdade de Direito da Universidade Lusíada). Repositório das Universidade Lusíada. <http://hdl.handle.net/11067/6548>

Russell, S. J., & Norvig, P. (2021). *Artificial Intelligence: A Modern Approach*. Pearson Education Limited

Saias J., M. Maia, L. Rato e T. Gonçalves (2018). Machine Learning: um estudo sobre conceitos, tarefas e algoritmos relacionados com predição e recomendação. Relatório Técnico. APRA-CP v2. <http://hdl.handle.net/10174/30174>

Santos, A.T. (2023). Investigação Criminal e a Inteligência Artificial: magia digital ou uma miragem?. *Revista do Ministério Público*, 175, 207-221.

SEARLE, John. "Minds, Brains, and Programs." *Behavioral and Brain Sciences*, 3(3), 417–457. <https://doi.org/10.1017/S0140525X00005756>

Silva, V.M.F. (2023). *A Inteligência Artificial Na Videovigilância – Benefícios e Riscos Associados – O Papel da PSP No Controlo do Sistema*. (Trabalho Individual Final do Curso

de Comando e Direção Policial, Instituto Superior de Ciências Policiais e Segurança Interna). RCAAP. <http://hdl.handle.net/10400.26/46018>

Singh, A., Aseri, V., Nagar, V., Lohar, S. (2024). Artificial Intelligence in Fingerprint Identification. *Artificial Intelligence in Forensic Science*, (p. 30-42). <http://10.4324/9781003287810-3>

Soares, F.J.L.R. (2024). *O Estado da Arte da Aplicação da Inteligência Artificial (IA) e a Aprendizagem Automática (AA) ao Cálculo de Estrutura*. (Dissertação de Mestrado, Faculdade de Engenharia da Universidade do Porto), Repositório Aberto da Universidade do Porto. <https://hdl.handle.net/10216/162129>

Sobreira, V. (2025). Um panorama da História da Inteligência Artificial e suas aplicações na pesquisa histórica. *Varia História*, 41(25035), 1-32. <https://doi.org/10.1590/0104-87752025v41e25035>

Souza, J.H. (2022). *Machine Learning: sua utilização e desafios*. (Trabalho de conclusão de curso de engenharia computacional, Faculdade Anhanguera), Repositório cognia. <https://repositorio.pgsscogna.com.br/handle/123456789/745>

Tirado, J. & Maurício, D. (2020). Bruise dating using deep learning. *Journal of Forensic Sciences*, 66 (1). <https://doi.org/10.1111/1556-4029.14578>

Torrão, A.A. (2024). *A importância da Polícia Científica No Seio Da Investigação Criminal Em Portugal*. (Dissertação de Mestrado, Universidade de Coimbra). RCAAP. <https://hdl.handle.net/10316/117408>

Ulbricht, L. & Egbert, S. (2024). In Palantir we trust? Regulation of data analysis platforms in public security. *Big Data & Society*, 11(3), 1-15. <https://doi.org/10.1177/20539517241255108>

Valente, M.M.G. (2003). *Regime jurídico da investigação criminal: comentado e anotado*. Almedina.

Valério, J. (2022). *Inteligência Artificial: A Origem*.
<https://diferencial.tecnico.ulisboa.pt/ciencia/inteligencia-artificial-a-origem-1-7/>

Valério, J. (2022). *Inteligência Artificial: Porquê Agora?*.
<https://diferencial.tecnico.ulisboa.pt/ciencia/inteligencia-artificial-porque-agora-2-7/>

Vicente, C.G.S.N. (2020). *Machine Learning Algorithms – Application on Big Data to Predict Retention Actions Needs*. (Dissertação de Mestrado Faculdade de Ciências e Tecnologias da Universidade Nova de Lisboa), RCAAP. <http://hdl.handle.net/10362/103843>

Wong, W. (2018). *VALCRI. PROJECT PERIODIC REPORT: FINAL COVERING PERIODS 1-3, MAY 2014 – JUNE 2018 (M01-M50)*. [final1-valcri-periodic-report-3-28-jun-2018.pdf](http://hdl.handle.net/10362/103843)