

MESTRADO
MEDICINA LEGAL

Parceria Humano-IA: Uma Investigação sobre a Integração Ótima da Inteligência Artificial em Processos de Justiça Criminal e Forenses

Cátia Soraia Tinoco da Silva

M

2025



Cátia Soraia Tinoco da Silva. Parceria Humano-IA: Uma Investigação sobre a Integração Ótima da Inteligência Artificial em Processos de Justiça Criminal e Forenses



M.ICBAS.2025

Parceria Humano-IA: Uma Investigação sobre a Integração Ótima da Inteligência Artificial em Processos de Justiça Criminal e Forenses
Cátia Soraia Tinoco da Silva



Cátia Soraia Tinoco da Silva

**Parceria Humano-IA: Uma Investigação sobre a Integração
Ótima da Inteligência Artificial em Processos de Justiça
Criminal e Forenses**

Dissertação de Candidatura ao grau
de Mestre em Medicina Legal
submetida ao Instituto de Ciências
Biomédicas de Abel Salazar da
Universidade do Porto.

Orientador – Doutor André Lamas
Leite

Afiliação – Faculdade de Direito da
Universidade do Porto

Coorientador – Doutora Maria da
Graça Borges Lobo

Afiliação – Instituto de Ciências
Biomédicas Abel Salazar

12 de setembro de 2025

Para os meus pais

Agradecimentos

Antes de mais, quero agradecer ao Professor André Lamas Leite por toda a orientação e, principalmente, pela paciência nos últimos dois meses desta corrida final. O seu apoio foi essencial para conseguir chegar à meta.

Um grande obrigado também à Professora Graça Lobo, não só por ter coorientado esta dissertação, mas também pelo acompanhamento constante e tão próximo durante o primeiro ano do mestrado. Fez mesmo a diferença.

Aos meus pais, obrigada por tudo: pelo incentivo constante, pelos valores e ética profissional que me transmitiram, e por nunca questionarem (pelo menos em voz alta) a ideia de fazer dois mestrados (e um MBA) seguidos. Mesmo quando parecia que eu já tinha desistido da dissertação (e da minha sanidade), vocês estiveram aqui.

Aos meus mais próximos — Guedes, Lili, Lulu e Babs —, obrigada por existirem, por me apoiarem em tudo, por me aturarem em todas as fases (inclusive as caóticas), e por me lembrarem que a vida não é só dissertações e *deadlines*.

Às "Catrafonas em Série", obrigada por terem tornado este segundo mestrado numa segunda juventude universitária. Obrigada por todas as gargalhadas, desabafos, dramas e momentos de pura galhofa académica.

E, por fim... a mim. Sim, a mim mesma. Porque escrever uma dissertação não é tarefa fácil, e se cheguei até aqui, foi porque (mesmo entre procrastinações, cafés, choradinhos e ataques de pânico existencial) continuei a aparecer, a escrever, a tentar. Esta vitória também é minha — e merecida.

Obrigada a todas e a todos.

If a machine is expected to be infallible, it cannot also be intelligent.

- Alan Turing, Palestra para a Sociedade Matemática de Londres, 1947

Lista de siglas e abreviaturas

AGI – Inteligência Artificial Geral (*Artificial General Intelligence*)

AI Act – Regulamento Europeu de Inteligência Artificial (*Artificial Intelligence Act*)

ANI – Inteligência Artificial Estreita (*Artificial Narrow Intelligence*)

COMPAS – *Correctional Offender Management Profiling for Alternative Sanction*

GenAI – Inteligência Artificial Generativa (*Generative Artificial Intelligence*)

IA – Inteligência Artificial

IoT – *Internet of Things* (Internet das Coisas)

Índice

Agradecimentos	3
Lista de siglas e abreviaturas	5
Resumo	7
Abstract	8
Introdução	9
1.1. Definição e Enquadramento Conceptual	13
1.2 Enquadramento Legal	15
2. Visão Geral das Aplicações da IA	20
2.1 IA na Investigação Criminal, Medicina Legal e Ciências Forenses	21
2.2 IA no processo penal, direito e justiça	27
3. Modelos de colaboração Humano-IA: o que existe?	30
4. Desafios e questões éticas	34
5. A integração ótima: reflexões e discussão	36
6. Conclusão	39
Referências	42
Bibliografia citada	42
Ferramentas, notícias e outras fontes	44
Legislação nacional e internacional	45

Resumo

A crescente utilização da inteligência artificial (IA) na justiça criminal e investigações forenses está a transformar profundamente a forma como lidamos com a descoberta de quem praticou crimes. Através da análise de grandes volumes de dados e da identificação de padrões complexos, a IA oferece novas ferramentas para auxiliar na investigação e na tomada de decisões judiciais. No entanto, é crucial destacar a importância da colaboração entre estas tecnologias e as perícias humanas tradicionais. A combinação do conhecimento especializado dos peritos com as capacidades analíticas das máquinas pode fornecer uma abordagem mais completa e eficaz para garantir a justiça e a precisão nos processos criminais. É ainda fundamental reconhecer os desafios e preocupações éticas associados à integração da IA em investigações criminais. Embora estas tecnologias ofereçam benefícios significativos, também levantam questões importantes sobre privacidade, viés algorítmico e transparência. É essencial garantir que o seu uso respeita os direitos individuais e os princípios éticos, além de ser transparente e responsável. A colaboração entre especialistas em ética, juristas e *developers* é fundamental para encontrar soluções que equilibrem a inovação tecnológica com a proteção dos direitos humanos e a justiça. Esta dissertação tem como objetivo explorar teoricamente esta integração e colaboração, a avaliação das vantagens e limitações das aplicações atuais de IA em investigações criminais, e a consciencialização em torno das considerações éticas e possíveis viés.

Palavras-chave: inteligência artificial, justiça criminal, ciências forenses, investigação criminal, ética.

Abstract

The increasing use of artificial intelligence (AI) in criminal justice and forensic investigations is profoundly transforming the way we handle crime resolution. By analysing large volumes of data and identifying complex patterns, AI provides new tools to assist in investigations and judicial decision-making. However, it is crucial to emphasize the importance of collaboration between these technologies and traditional human expertise. The combination of specialists' knowledge with the analytical capabilities of machines can offer a more comprehensive and effective approach to ensuring justice and accuracy in criminal proceedings. It is also essential to recognize the challenges and ethical concerns associated with integrating AI into criminal investigations. While these technologies offer significant benefits, they also raise important questions about privacy, algorithmic bias, and transparency. Ensuring that AI usage respects individual rights and ethical principles, while being transparent and accountable, is fundamental. Collaboration among ethics experts, legal professionals, and developers is key to finding solutions that balance technological innovation with the protection of human rights and justice. This dissertation aims to explore the theoretical aspects of this integration and collaboration, evaluate the advantages and limitations of current AI applications in criminal investigations, and consider the ethical concerns and potential biases involved.

Keywords: artificial intelligence, criminal justice, forensic sciences, criminal investigation, ethics.

Introdução

A era digital e o avanço tecnológico do século XXI levaram ao crescimento exponencial do acesso, pela pessoa comum, à informação livre. Com a criação de novos e cada vez mais inteligentes motores de busca, redes sociais, presença *online* da comunicação social/*media*, foi natural e esperada a evolução do sistema de justiça, do Direito, e dos métodos da investigação criminal, no sentido de acompanhar esta mudança do paradigma social. Esta evolução incluiu, no que tange à justiça, não só a digitalização das decisões judiciais, mas também a sua disponibilização *online* e, consequentemente, o acesso facilitado e generalizado à jurisprudência dos Tribunais superiores, embora tarde em cumprir-se a promessa de sucessivos Governos no sentido de também serem colocados ao dispor de todos as decisões dos Tribunais de 1.^a instância (sentenças e acórdãos).

Foi apenas uma questão de tempo até este acesso livre impulsionar o desenvolvimento e uso de ferramentas computacionais, desde sistemas simples até algoritmos avançados, capazes de analisar decisões judiciais prévias e prever decisões futuras, através da identificação de padrões. Antes destas ferramentas — que vieram a ser definidas como modelos de aprendizagem automática, capazes de extrair padrões a partir de grandes volumes de dados e adaptar-se com base na experiência acumulada —, estes sistemas funcionavam com regras fixas, do tipo *If this, than that*¹. Passamos a estar perante modelos imitadores de processos cognitivos humanos.

Embora nem todas as decisões do ser humano sejam resultado de um processo racional, todas elas seguem, sem exceção, certos princípios cognitivos, que não são possíveis para um sistema de inteligência artificial (IA), para já incapaz de entender as reações humanas².

Atualmente, as máquinas, os programas e os sistemas de IA requerem intervenção humana, e mesmo os sistemas de IA mais “inteligentes” e avançados cometem erros. Os sistemas são apenas tão inteligentes quanto a informação de que se alimentam e usada na sua aprendizagem, razão pela qual o seu uso para, por

¹ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, in Anabela Miranda Rodrigues (coord.), *A Inteligência Artificial no Direito Penal*, Coimbra: Edições Almedina, 2022, pp. 11-58.

² Gustavo Mascarenhas Lacerda Pedrina, *Consequências e perspectivas da aplicação de inteligência artificial a casos penais*, *Revista Brasileira de Direito Processual Penal*, vol. 5, n.º 3, 2019, pp. 1589-1606. Disponível em: <https://doi.org/10.22197/rbdpp.v5i3.265> [Acesso em: abril de 2024].

exemplo, redigir uma decisão judicial pode ser problemática se as decisões passadas contiverem viés, uma vez que estes vão ser reconhecidos pelo sistema como regras, tornando todo o sistema enviesado³.

É, portanto, importante reconhecer, antes de proceder com esta investigação e teorização acerca de uma possível “integração ótima da inteligência artificial em processos de justiça criminal e forenses”, que a probabilidade de um sistema de IA chegar a uma decisão judicial injusta, por exemplo, é significativa, pois este não será capaz de considerar holisticamente a situação. O mesmo podemos dizer da capacidade do sistema considerar criticamente provas forenses, num processo de investigação criminal.

O uso da IA na prova digital em processo penal impõe a reavaliação de questões essenciais. É legítima uma intrusão tão profunda na privacidade e intimidade? Está salvaguardado o pleno exercício do direito de defesa do arguido? Poderá a lei processual penal vigente ser interpretada de forma a permitir o uso de sistemas de IA no interesse da investigação? Embora estas tecnologias possam aumentar a eficácia no combate à criminalidade, não é certo que conduzam a uma justiça mais equitativa. O desafio, que se renova sob novas formas, consiste em alcançar o equilíbrio entre a eficiência exigida à justiça penal e a proteção dos direitos fundamentais, sobretudo os do arguido⁴.

Ainda nos encontramos na considerada 1.^a fase da IA, reconhecida na literatura como “Artificial Narrow Intelligence”, ou *ANI* (Inteligência Artificial Estreita). Esta fase inclui sistemas com os quais estamos familiarizados e que a pessoa comum encontra diariamente, desde os reconhecimentos faciais e de voz que usamos nos nossos telemóveis e redes sociais, aos veículos com condução autónoma que têm surgido. Esta fase permite apenas o uso da IA em áreas específicas, sendo o sistema programado para uma tarefa específica e incapaz de resolver problemas de outras áreas autonomamente. No entanto, está programado

³ Andreas Kaplan e Michael Haenlein, *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, *Business Horizons*, vol. 62, nr. 1 Jan.–Feb. 2019, pp. 15-25. Disponível em: <https://doi.org/10.1016/j.bushor.2018.08.004> [Acesso em: maio de 2025]; Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, *op. cit.*, p. 11-58.

⁴ Sónia Fidalgo, A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo, in Anabela Miranda Rodrigues (coord.), *A Inteligência Artificial no Direito Penal*, *op. cit.*, pp. 129-161.

para equiparar ou ultrapassar a *performance* do ser humano na(s) tarefa(s) para o qual foi desenhado⁵.

Vislumbres da 2.^a fase — “Artificial General Intelligence”, ou *AGI* (Inteligência Artificial Geral) — já se fazem sentir com a introdução da “Inteligência Artificial Generativa” (ou *GenAI*)⁶. A *AGI* permitirá que os sistemas raciocinem e executem tarefas autonomamente, sem ser necessária a sua programação. Nesta fase, o sistema de IA será equiparado ao ser humano, capaz de ultrapassar a *performance* deste último em várias áreas⁷.

Num futuro mais ou menos próximo, dependendo da velocidade do desenvolvimento tecnológico, iremos alcançar uma 3.^a fase, a que os autores têm dado o nome de “Artificial Super Intelligence”, com os sistemas a atingirem a autoconsciência. Nesta, prevê-se que o sistema de IA será superior ao ser humano em todas as áreas⁸.

No seu artigo “Siri, Siri, in my hand”, publicado em 2019⁹, Kaplan e Haenlein usam a *Siri*, Assistente de IA do *iPhone*, para exemplificar as três fases acima descritas: na 1.^a fase, a *Siri* é capaz de reconhecer a voz do operador, mas é incapaz de executar qualquer outra tarefa, como conduzir um carro; na 2.^a fase, a *Siri* evolui para um robô com características humanas, capaz não só de reconhecer a voz do operador, mas também preparar-lhe um café, e escrever; na 3.^a fase, a *Siri* desenvolve capacidades sobre-humanas, tornando-se capaz de resolver problemas matemáticos complexos instantaneamente, e escrever um *bestseller* em segundos.

Aqui poderá ser pertinente refletir sobre o conceito de “inteligência”, sendo que vários autores, incluindo Kaplan e Haenlein, referem que o caminho mais comum para definir a IA é usando a “inteligência humana” como referência.

⁵ Andreas Kaplan e Michael Haenlein, *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, op. cit., pp. 15-25. Disponível em: <https://doi.org/10.1016/j.bushor.2018.08.004> [Acesso em: maio de 2025]; Túlio Xavier Januário, *Inteligência Artificial e Direito Penal da Medicina*, in Anabela Miranda Rodrigues (coord.), *A Inteligência Artificial no Direito Penal* (Vol. II), op. cit., pp. 125-173.

⁶ Subcampo da IA que utiliza modelos generativos para produzir texto, imagens, vídeos ou outras formas de dados, através da aprendizagem de padrões e estruturas subjacentes dos dados com que foram treinados, e o subsequente uso dos mesmos para gerar novos dados. Adam Pasick, Artificial Intelligence Glossary: Neural Networks and Other Terms Explained. *The New York Times* [online]. Disponível em: <https://www.nytimes.com/article/ai-artificial-intelligence-glossary.html> [Acesso em junho de 2025].

⁷ Andreas Kaplan e Michael Haenlein, *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, *Business Horizons*, op. cit.; Túlio Xavier Januário, *Inteligência Artificial e Direito Penal da Medicina*, op. cit., pp. 125-173.

⁸ *Idem*.

⁹ *Idem*.

O dicionário português *Priberam* define “inteligência”¹⁰ como o “conjunto de todas as faculdades intelectuais (memória, imaginação, juízo, raciocínio, abstração e conceção)”. Já o dicionário inglês de Oxford define *intelligence*¹¹ em várias vertentes, incluindo: 1) “The faculty of understanding; intellect”¹²; 2) “The action or fact of mentally apprehending something; understanding, knowledge, comprehension (of something)”¹³; 3) “An intelligent or rational being”¹⁴. Esta última definição de Oxford é, possivelmente, a razão de ser de toda a discussão em torno da IA e da sua capacidade de “substituir” o ser humano em certas circunstâncias, incluindo na tomada de decisões.

No campo da justiça e da investigação criminal, o conceito de “inteligência” assume antes um papel instrumental, configurando dados recolhidos e analisados com o objetivo de produzir conhecimento útil à tomada de decisões¹⁵, ou, citando novamente o dicionário português *Priberam*, a “atividade ou serviço que visa obter e fornecer informações secretas relativas ao Estado, ao governo, à segurança ou a setores estratégicos”¹⁶. O dicionário inglês de Oxford inclui também esta perspetiva entre as suas várias definições de inteligência, que atribui aos vários séculos de uso desde a sua etimologia.

Resumidamente, a inteligência pode ser entendida como o processo de recolher, organizar e analisar informação com vista à satisfação de determinadas finalidades e, até recentemente, associava-se esta qualidade excecionalmente ao funcionamento cognitivo humano.

¹⁰ “Inteligência”, *Dicionário Priberam da Língua Portuguesa* [online]. Disponível em: <https://dicionario.priberam.org/intelig%C3%A2ncia> [Acesso em: maio de 2025].

¹¹ “Intelligence”, *Oxford English Dictionary* [online]. Disponível em: https://www.oed.com/dictionary/intelligence_n?tab=meaning_and_use&tl=true#214347 [Acesso em: maio de 2025].

¹² Em português, “A capacidade de compreensão; intelecto”.

¹³ Em português, “A ação ou facto de apreender mentalmente algo; entendimento, conhecimento, compreensão (de algo)”.

¹⁴ Em português, “Um ser inteligente ou racional”.

¹⁵ Fernanda Silva Lobato, *Uso de softwares com função analítica preditiva aplicados à investigação criminal e atividade de inteligência: uma análise sobre o conflito de normas relativas ao direito constitucional à privacidade e à segurança pública*, Trabalho de Conclusão de Curso, Instituto de Ciências Jurídicas, Faculdade de Direito, Universidade Federal do Pará, 2019. Disponível em: <https://bdm.ufpa.br/items/a14265d7-375b-4606-af54-c99e960ceffa/full> [Acesso em: abril de 2024].

¹⁶ “Inteligência”, *Dicionário Priberam da Língua Portuguesa* [online]. Disponível em: <https://dicionario.priberam.org/intelig%C3%A2ncia> [Acesso em: maio de 2025].

1. A Inteligência Artificial na sua base

1.1. Definição e Enquadramento Conceptual

Definir IA revela-se difícil quando consideramos as diferentes definições e perspectivas contidas nos múltiplos artigos, livros e comunicações acerca da temática que foram consultados ao longo da elaboração desta investigação. Kaplan e Haenlein (2019)¹⁷ sugerem que a dificuldade em definir o que é (e o que não é) a IA pode advir da dificuldade em definir a própria inteligência (algo que já tentámos fazer na introdução a este trabalho). Outra razão apontada pelos mesmos autores é a rápida evolução da tecnologia usada e da própria área de estudo, cuja velocidade é superior à dos estudos académicos que a tentam definir. As tecnologias que consideramos inovadoras há cinco ou dez anos já estão ultrapassadas.

O termo “inteligência artificial” aparenta ter como génese a década de 50 do século passado, com o cientista John McCarthy¹⁸, ressaltando, no entanto, a forte e importante influência e contribuição de Alan Turing como ponto de partida à exploração da temática e da sua possibilidade, como salientou em 2022 Túlio Xavier Januário¹⁹.

Em “Computing Machinery and Intelligence”²⁰, publicado por Turing em 1950, o autor previu a 2.ª fase da IA:

In this sort of sense, a machine undoubtedly can be its own subject matter. It may be used to help in making up its own programmes, or to predict the effect of alterations in its own structure. By observing the results of its own behaviour, it can modify its own programmes so as to achieve some purpose

¹⁷ Andreas Kaplan e Michael Haenlein, *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, *Business Horizons*, op. cit..

¹⁸ O termo pode ser encontrado no texto referente a uma proposta de investigação datada de 31 de agosto de 1955 (“A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence”), da autoria de John McCarthy, Marvin L. Minsky, Nathaniel Rochester e Claude E. Shannon. Esta proposta foi, mais tarde, em 2006, publicada na *AI Magazine*, 27(4), 12, ainda disponível em <https://doi.org/10.1609/aimag.v27i4.1904>; Andreas Kaplan e Michael Haenlein, *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, op. cit..

¹⁹ Túlio Xavier Januário, *Inteligência Artificial e Direito Penal da Medicina*, op. cit..

²⁰ Alan M. Turing, *Computing Machinery and Intelligence*. *Mind*. Vol. 59, nr. 236 (Oct. 1950), pp. 433-460. Disponível em: <https://doi.org/10.1093/mind/LIX.236.433>. [Acesso em: maio de 2025].

*more effectively. These are possibilities of the near future, rather than Utopian dreams.*²¹

Atualmente, podemos entender a IA como uma área especializada da ciência da computação que visa o desenvolvimento de sistemas capazes de reproduzir funções cognitivas humanas, tais como a aprendizagem, o raciocínio, a adaptação e a autocorreção. Em “Direito da Informática”²², Marques e Martins definiram simplificadaamente a IA como o “conjunto de técnicas utilizadas para conceber programas que simulem o funcionamento do raciocínio humano na resolução de determinados problemas complexos”.

Estes sistemas são concebidos para executar tarefas difíceis, como o reconhecimento visual, o processamento de linguagem natural, a tomada de decisões e a resolução de problemas, com níveis elevados de precisão e eficiência.²³ No contexto da justiça criminal e forense, como iremos averiguar ao longo desta investigação, a IA pode assumir, e em alguns contextos assume já, um papel crescente no apoio à investigação, na gestão de grandes volumes de dados e na tomada de decisões no contexto judicial.

Conceptualmente, a IA configura uma área abrangente com subdomínios que se interrelacionam, como o *machine learning* e o *deep learning*. O *machine learning* permite que o sistema computacional aprenda com base em dados históricos e reconheça padrões sem ser prévia e explicitamente programado para tal. Já o *deep learning*, uma vertente mais avançada, funciona com base numa estrutura em rede que imita o funcionamento do cérebro humano²⁴.

É importante referir a distinção entre a IA e os conceitos de *Internet of Things* (IoT) e *big data*. Podemos definir *IoT* como um dos métodos de obtenção de dados externos, dados esses que são subsequentemente alimentados aos sistemas de IA

²¹ Em português, “Neste sentido, uma máquina pode, sem dúvida, ser o seu próprio objeto de estudo. Pode ser utilizada para ajudar a criar os seus próprios programas ou para prever o efeito de alterações na sua própria estrutura. Ao observar os resultados do seu próprio comportamento, pode modificar os seus próprios programas de forma a atingir um determinado objetivo com maior eficácia. Estas são possibilidades de um futuro próximo, e não sonhos utópicos”.

²² Garcia Marques e Lourenço Martins, *Direito da Informática*. Coimbra: Almedina, 2000, pp. 1-771.

²³ Ekta B. Jadhav, Mahipal Singh Sankhla e Rajeev Kumar, *Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation*, *Seybold Report*, 2020, vol. 15, pp. 2064-2075. Disponível em:

https://www.researchgate.net/publication/343826071_Artificial_Intelligence_Advancing_Automation_in_Forensic_Science_Criminal_Investigation [Acesso em: maio de 2025]

²⁴ *Idem*.

(*input*), e *big data* como a junção de vários *datasets* (incluindo a *IoT*) de grande dimensão, atualizados, e em diversos formatos (desde texto a vídeo). A IA funciona ao usar as informações da *IoT* e outras fontes de *big data* para identificar padrões e estabelecer regras através de *machine learning*. Este último é essencial à IA²⁵.

1.2 Enquadramento Legal

A grande maioria da legislação em torno do uso de sistemas de IA não se foca na implementação e alcance destes sistemas, mas sim na proteção dos dados pessoais dos utilizadores da *internet* (assim como dos direitos de autor), cujo conteúdo faz parte da *IoT* e do *big data*, usados para alimentar e treinar os sistemas de IA. Um exemplo bastante atual, mas que não se relaciona com a temática desta investigação, é a problemática do uso de *GenAI* para a criação de “arte” e/ou escrita criativa. Como se referiu anteriormente, os sistemas de IA atuais conseguem funcionar apenas através do uso de dados pré-existentes, que lhes são alimentados, para gerar as suas respostas. Significa isto que, para a geração de imagens, o sistema irá servir-se de arte pré-existente nas várias bases de dados *online*, um ato de “plagiarismo”²⁶ contra o qual vários artistas, desde as artes visuais à escrita, se têm pronunciado²⁷.

No entanto, estas tecnologias podem contribuir (e em algumas jurisdições já contribuem) para a criação de sistemas inteligentes capazes de apoiar o ser humano na tomada de decisões em ambientes de elevada complexidade, como é o caso do sistema de justiça penal, pelo que é necessário que exploremos, ainda que superficialmente, a legislação existente neste âmbito.

Em Portugal, até ao momento, não existe legislação nacional específica sobre IA *de per se*, talvez porque os Estados compreendam — e bem — que os desafios por ela colocados não se podem conter nas fronteiras de um deles, mas desbordam a sua

²⁵ Andreas Kaplan e Michael Haenlein, *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*, op. cit..

²⁶ Anglicismo derivado da palavra “plagiarism”.

²⁷ Vários artigos jornalísticos têm sido publicados acerca desta temática, incluindo: 1. Kevin Roose, *An A.I.-Generated Picture Won an Art Prize. Artists Aren't Happy*. *The New York Times* [online]. Publicado a 2 de setembro de 2022. Disponível em: <https://www.nytimes.com/2022/09/02/technology/ai-artificial-intelligence-artists.html> [Consultado em junho 2025]; 2. Nick Reilly, *Artists Score Major Win in Copyright Case Against AI Art Generators*. *Hollywood Reporter* [online]. Publicado a 13 de agosto de 2024. Disponível em: <https://www.hollywoodreporter.com/business/business-news/artists-score-major-win-copyright-case-against-ai-art-generators-1235973601/> [Consultado em junho 2025]; e 3. Clare Hutchinson e Phil John, *AI: Digital Artist's Work Copied More Times Than Picasso*. *BBC News* [online]. Publicado a 20 de julho de 2023. Disponível em: <https://www.bbc.com/news/uk-wales-66099850> [Consultado em junho 2025].

utilização em todos os sistemas jurídicos. Daí que organizações internacionais de que Portugal faz parte sejam o fórum privilegiado para essa regulação, o que já existe.

O Regulamento Europeu de Inteligência Artificial (*AI Act*), de 13 de junho de 2024²⁸, foi concebido com vista a criar um regime jurídico uniforme para o desenvolvimento e utilização de sistemas de IA, promovendo uma IA centrada no ser humano e alinhada com os valores da UE. De acordo com as regras do Direito da União Europeia derivado, os regulamentos são uma forma de legislar em que as autoridades dos Estados-membros se limitam a aplicar e a fiscalizar o cumprimento desses normativos, uma vez que, ao contrário das diretivas, por exemplo, são dotados de aplicabilidade direta e de eficácia direta, sendo obrigatórios em todo o seu conteúdo, vinculando pessoas singulares e coletivas e, dependendo da matéria, pessoas de Direito Público e de Direito Privado, não carecendo de qualquer ato legislativo de transposição. Tudo se passa como se estivéssemos a falar de uma lei nacional (em sentido amplo) que, decorrido o prazo da *vacatio legis*, vincula todos aqueles a que se destina, exatamente da forma como se acha recolhida no diploma, podendo, em consequência, servir como fundamento de ações judiciais em caso de incumprimento.

No Capítulo I das Disposições Gerais, art. 1.º, n.º 2, o *AI Act* estabelece primeiramente, que um dos seus objetivos é a criação de “regras harmonizadas para a colocação no mercado, a colocação em serviço e a utilização de sistemas de [IA] na União” (al. a)), assim como de “proibições de certas práticas de [IA]” (al. b)). Para o propósito desta investigação, que se foca no uso da IA na investigação e justiça criminal, o disposto na al. b) é especialmente relevante. O *AI Act* discorre acerca das práticas de IA proibidas no seu Capítulo II, contendo apenas um comando legal (art. 5.º), com o objetivo de proteger os direitos fundamentais e garantir uma utilização ética da IA. Essas proibições, constantes do n.º 1, alíneas a) a h), do art. 5.º, resumem-se ao seguinte:

- a) É proibida a utilização de sistemas de IA que recorram a técnicas subliminares ou manipuladoras, com o objetivo ou efeito de distorcer o comportamento de indivíduos ou grupos, contornando a sua consciência;
- b) Não são permitidos sistemas de IA que explorem vulnerabilidades decorrentes da idade, incapacidade ou condição socioeconómica, sempre

²⁸ Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 - Regulamento Europeu de Inteligência Artificial (*AI Act*). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689. Consultado a 27 de junho de 2025.

que tal exploração vise ou tenha como efeito a distorção significativa do comportamento, causando ou podendo causar danos relevantes;

c) É vedado o uso de sistemas de IA para avaliar ou classificar pessoas singulares ou grupos com base no comportamento social ou em características pessoais, sempre que tal classificação resulte em tratamento discriminatório ou desproporcionado em contextos não diretamente relacionados com os dados recolhidos;

d) São proibidos sistemas de IA que realizem avaliações de risco de infrações penais com base exclusiva em perfis ou traços de personalidade, salvo quando utilizados como apoio à avaliação humana fundamentada em factos objetivos e verificáveis;

e) Não é permitido o desenvolvimento ou expansão de bases de dados de reconhecimento facial através da recolha indiscriminada de imagens da *internet* ou de sistemas de videovigilância;

f) São proibidos sistemas de IA que pretendam inferir emoções em locais de trabalho ou instituições de ensino, exceto quando destinados a fins médicos ou de segurança devidamente justificados;

g) É interdita a categorização biométrica que permita deduzir características sensíveis como origem racial, convicções religiosas, opiniões políticas, filiação sindical ou orientação sexual, entre outras e

h) A utilização de sistemas de identificação biométrica em tempo real em espaços públicos para aplicação da lei é proibida, salvo em situações estritamente necessárias e delimitadas, como busca de vítimas de crimes graves ou desaparecidas, prevenção de ameaças iminentes à vida ou à

integridade física, e localização de suspeitos de crimes graves puníveis com pena privativa de liberdade igual ou superior a quatro anos²⁹.

As alíneas d) e h) são aqui particularmente relevantes, mais uma vez, dado o contexto e objetivo do presente estudo.

Ainda sobre o *AI Act*, é relevante mencionar que ele divide os diferentes sistemas de IA em quatro níveis de risco: mínimo, limitado, alto e inaceitável, sendo que os sistemas usados em recrutamento, justiça e policiamento são classificados como de alto risco.

O Capítulo III, Secção I estabelece a “Classificação de sistemas de IA como sendo de risco elevado”. Segundo o seu art. 6.º, n.º 2, todos os sistemas de IA a que se refere o Anexo III devem ser classificados como sendo de risco elevado. Por outro lado, o seu n.º 3 estabelece que um sistema referido no Anexo III apenas será de risco elevado se “representar um risco significativo de danos para a saúde, a segurança ou os direitos fundamentais das pessoas singulares”, e se influenciar tomadas de decisão. Adicionalmente, o n.º 3 estabelece que os sistemas do Anexo III “devem ser sempre considerados de risco elevado nos casos em que executarem a definição de perfis de pessoas singulares”, sem prejuízo do disposto na primeira parte do n.º 3.

Ora, por si só, o n.º 3 aparenta ter implicações significativas no que concerne à temática desta investigação, pelo que olharemos agora para o conteúdo do Anexo III.

Este último divide os sistemas de risco elevado em oito domínios, sendo que aqueles que guardam aparente relevância para a presente investigação são os n.ºs 6 e 8, respetivamente: “Aplicação da lei, na medida em que a sua utilização seja permitida nos

²⁹ Em específico no que toca à alínea h), a aplicabilidade dos sistemas de identificação biométrica nas situações descritas carece, desde logo, do preenchimento de requisitos legais previstos nos n.ºs 2 e 3 do mesmo inciso, incluindo a sua estrita aplicabilidade à confirmação da identidade de uma pessoa antes já identificada, a natureza da situação concreta (nomeadamente a gravidade, a probabilidade e a magnitude dos danos evitáveis) e o impacto potencial sobre os direitos e liberdades das pessoas afetadas. Adicionalmente, o seu uso requer uma autorização prévia por parte de uma autoridade judiciária ou de uma autoridade administrativa independente com competência vinculativa, sendo que, em situações de urgência devidamente justificadas, se admite a ativação sem autorização prévia, desde que esta seja solicitada no prazo máximo de 24 horas. Caso a autorização seja recusada, a utilização deve cessar de imediato e todos os dados recolhidos devem ser eliminados, no que se aproxima legalmente do que vem sendo designado por *exclusionary rules* nos EUA e por *Beweisverboten* no sistema criminal alemão, este último exercendo uma significativa influência sobre o legislador, a doutrina e a jurisprudência nacionais (“proibições de prova”: entre outros, cf. art. 126.º do Código de Processo Penal).

termos do Direito da União ou do Direito nacional aplicável” e “Administração da justiça e processos democráticos”³⁰.

Olhemos mais aprofundadamente para o n.º 6. Nos seus termos, são identificados como sistemas de alto risco aqueles que são concebidos para fins de aplicação da lei, desde que a sua utilização seja permitida pelo Direito da UE ou nacional. Estes incluem sistemas destinados a avaliar o risco de vitimização criminal, operar como polígrafos ou instrumentos análogos, aferir da fiabilidade de provas no decurso de investigações, prever o risco de cometimento de infrações ou reincidência (desde que não baseados exclusivamente em perfis pessoais), bem como sistemas que definem perfis no contexto da investigação e repressão criminal. O próprio *AI Act* proíbe algumas destas práticas, como anteriormente mencionado.

Importa refletir sobre os desafios éticos e jurídicos subjacentes à inclusão destes sistemas no grupo de alto risco. Embora o legislador europeu reconheça o seu potencial instrumental no apoio à justiça penal, a sua utilização implica riscos significativos para os direitos fundamentais, desde a presunção de inocência até à não discriminação, tudo valores com assento na Carta de Direitos Fundamentais da União Europeia³¹ e nas Constituições de todos os 27 Estados-membros (no nosso caso, respetivamente, os artigos 32.º, n.º 2, e 13.º, da Constituição da República Portuguesa³²). A dependência de sistemas automatizados na produção de avaliações de risco ou na análise probatória pode comprometer princípios fundamentais do processo penal como o contraditório e a imparcialidade. Além disso, a definição e utilização de perfis, ainda que legalmente enquadradas, levantam questões quanto à transparência, à possibilidade de enviesamentos algorítmicos e à replicação de desigualdades sociais. Neste sentido, a categorização destes sistemas como de “alto risco” revela-se adequada, mas insuficiente, se não for acompanhada de mecanismos robustos de escrutínio, responsabilização e auditoria contínua. Estas questões serão aprofundadas na Parte III da presente

³⁰ Os restantes domínios são: 1. Dados biométricos; 2. Infraestruturas críticas (componentes de segurança na gestão e no controlo de infraestruturas digitais críticas, do trânsito rodoviário ou das redes de abastecimento de água, gás, aquecimento ou eletricidade); 3. Educação e formação profissional; 4. Emprego, gestão de trabalhadores e acesso ao emprego por conta própria; 5. Acesso a serviços privados essenciais e a serviços e prestações públicos essenciais; e 7. Gestão da migração, do asilo e do controlo de fronteiras.

³¹ *Carta dos Direitos Fundamentais da União Europeia*. Jornal Oficial da União Europeia, C 326, 26 de outubro de 2012, p. 391-407. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12012P%2FTXT>. Consultada a 3 de agosto de 2025.

³² *Constituição da República Portuguesa*. 7.ª rev. Diário da República, 1.ª série, n.º 178, de 10 de setembro de 2005. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Consultada a 3 de agosto de 2025.

dissertação, onde se analisará o impacto da IA na investigação criminal e no funcionamento do sistema de justiça penal à luz dos princípios do Estado de Direito.

Como se disse acima, para além do Regulamento da União sobre a matéria, o legislador português aprovou a Carta Portuguesa dos Direitos Humanos na Era Digital, através da Lei n.º 27/2021, de 17 de maio³³, entretanto alterada pela Lei n.º 15/2022, de 11 de agosto.

O seu art. 9.º destina-se ao “uso da inteligência artificial e de robôs” e está dividido em três aspetos, que podemos sumariar da seguinte forma: 1. A IA deve ser desenvolvida e utilizada com respeito pelos direitos fundamentais, assegurando um equilíbrio entre explicabilidade, segurança, transparência e responsabilidade, e prevenindo a discriminação; 2. As decisões automatizadas (com recurso a algoritmos) com impacto significativo nos destinatários devem ser comunicadas aos afetados, auditáveis e suscetíveis de recurso; 3. A criação e utilização de robôs devem respeitar os princípios da beneficência, não-maleficência, autonomia e justiça, bem como os valores constantes do art. 2.º³⁴ do Tratado da União Europeia³⁵. Em suma, a norma pretende garantir a proteção do cidadão contra decisões automatizadas.

2. Visão Geral das Aplicações da IA

A presença da IA na investigação criminal, no processo penal e na justiça já não é apenas uma hipótese futura: é uma realidade em construção. Mais do que uma simples evolução tecnológica, trata-se de uma transformação profunda na forma como se investigam crimes, se analisam provas e se tomam decisões. Se antes falávamos apenas de métodos de análise mais sofisticados, hoje lidamos com sistemas capazes de criarem e interpretarem dados de forma autónoma, sem intervenção humana direta. Isso significa que estas ferramentas não só podem ajudar na investigação, mas também podem vir a influenciar a decisão final de um tribunal. Tal cenário abre novas possibilidades — como a justiça preditiva ou a avaliação de risco e perigosidade —, mas também levanta questões

³³ Lei n.º 27/2021, de 17 de maio – Carta Portuguesa de Direitos Humanos na Era Digital (3.ª versão). Disponível em https://pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3446&tabela=leis&so_miolo=. Consultada a 27 de junho de 2025.

³⁴ Passando a citar: “Artigo 2.º - A União funda-se nos valores do respeito pela dignidade humana, da liberdade, da democracia, da igualdade, do Estado de direito e do respeito pelos direitos do Homem, incluindo os direitos das pessoas pertencentes a minorias. Estes valores são comuns aos Estados-Membros, numa sociedade caracterizada pelo pluralismo, a não discriminação, a tolerância, a justiça, a solidariedade e a igualdade entre homens e mulheres.”

³⁵ Tratado da União Europeia de 2007. Disponível em <https://dcjri.ministeriopublico.pt/sites/default/files/documentos/instrumentos/rar40-1992.pdf>. Consultado a 27 de junho de 2025.

fundamentais sobre a proteção das garantias de defesa, a transparência das provas e a preservação do elemento humano no ato de julgar.

2.1 IA na Investigação Criminal, Medicina Legal e Ciências Forenses

A investigação criminal é um processo sistemático e articulado, conduzido, em Portugal, por autoridades judiciais e por órgãos de polícia criminal, com o propósito de apurar a verdade dos factos, identificar os autores de um crime e determinar as suas consequências, envolvendo a recolha, análise e interpretação de dados com, não apenas rigor técnico, mas também sensibilidade contextual, experiência prática e adaptação a realidades complexas.³⁶

Tradicionalmente, este processo inicia-se com a receção da *notitia criminis* ou com a análise da cena do crime. A partir daí, desenrola-se o percurso investigativo apoiado em métodos e procedimentos formalizados e dependente da capacidade dos investigadores para interpretar os indícios e atribuir-lhes significado, usando a lógica dedutiva e a reconstrução sequencial dos factos. Sendo assim, a investigação está sujeita às limitações humanas, técnicas e institucionais, desde a escassez de recursos até à fragmentação da informação disponível, que a podem condicionar³⁷.

Historicamente, os Tribunais mostraram-se reticentes quanto à aceitação de determinados meios tecnológicos como instrumentos válidos para a produção de prova em sede de processo penal. Contudo, a realidade atual é profundamente distinta: grande parte das nossas atividades quotidianas deixam um rasto digital, armazenado em sistemas informáticos. Este novo contexto levanta inevitavelmente questões sobre o valor e o tratamento destes registos no âmbito judicial³⁸.

É compreensível o interesse das autoridades em acederem a tais sistemas para recolher elementos probatórios que permitam esclarecer a prática de crimes e identificar os seus autores. Ora, é expectável que este tipo de prova tenha progressivamente conquistado espaço nos Tribunais como meio legítimo de demonstração dos factos³⁹.

³⁶ Stefania Costantini, Giovanni De Gasperis e Raffaele Olivier, *Digital forensics and investigations meet artificial intelligence*, *Annals of Mathematics and Artificial Intelligence*, vol. 86, nr. 2 (2019), pp. 193-229, DOI: 10.1007/s10472-019-09632-y, publicado em 24 de abril de 2019.

³⁷ Stefania Costantini, Giovanni De Gasperis e Raffaele Olivier, *Digital forensics and investigations meet artificial intelligence*, *op. cit.*; Yung-Fou Chen e Paul Kuei-chi Tseng, *The Boundary of Artificial Intelligence in Forensic Science*. *DIALOGO* [online], Vol. 10, nr. 1 (2023), p. 49-60. Disponível em: <https://doi.org/10.51917/dialogo.2023.10.1.5>

³⁸ Sónia Fidalgo, A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo, *op. cit.*

³⁹ *Idem*.

A novidade da prova digital limitou-se ao formato do seu armazenamento, logo que os intervenientes processuais se conseguiram adaptar sem grandes obstáculos. No entanto, a contínua e acelerada evolução tecnológica veio tornar a prova digital mais complexa, exigindo novos métodos de tratamento da informação. É aqui que as técnicas de IA têm desempenhado um papel crescente, oferecendo ferramentas mais avançadas de análise no domínio da ciência forense digital e ampliando a capacidade de processamento⁴⁰.

O conceito da *prova eletrónica* é mais abrangente que o de *prova digital*, na medida em que engloba não apenas a prova obtida através de dados em formato digital, mas também por meio de dados em formato analógico. A prova digital distingue-se por ser produzida a partir de dados em formato digital que são posteriormente manipulados, armazenados ou comunicados através de qualquer dispositivo, computador, ou sistema informático, ou transmitidos através de um sistema de comunicação. Entre as principais características da prova digital destacam-se a sua imaterialidade e invisibilidade. Estas características tornam-na especialmente vulnerável, pois a prova digital pode ser facilmente alterada, apagada ou destruída, seja pela ação de utilizadores, seja por mecanismos automáticos dos próprios sistemas operativos. Tal fragilidade levanta desafios à sua preservação e fiabilidade⁴¹.

A recolha e análise da prova são etapas fundamentais, nas quais se procura reconstruir eventos, sequências temporais e possíveis cenários com base em evidência empírica, e os seus resultados são essenciais ao processo-crime, servindo de base para a decisão judicial. Dentro desta lógica, e com a crescente digitalização da sociedade e da criminalidade, seria de esperar que houvesse uma movimentação para a introdução de mecanismos tecnológicos que pudessem auxiliar na gestão e análise da prova, no entanto, verifica-se que estas continuam a depender da intervenção manual de especialistas humanos⁴².

Porém, nos últimos anos, têm surgido no mercado diversas soluções tecnológicas de base comercial (*Commercial Off-The-Shelf*, ou *COTS*, por exemplo), destinadas ao apoio à investigação forense digital⁴³. O crescimento da capacidade dos sistemas de armazenamento digital e a sua presença constante na vida quotidiana têm provocado um

⁴⁰ *Idem*.

⁴¹ *Idem*.

⁴² Stefania Costantini, Giovanni De Gasperis e Raffaele Olivier, *Digital forensics and investigations meet artificial intelligence*, *op. cit.*.

⁴³ *Idem*.

aumento significativo no número de pedidos de recolha e análise de dados em processos penais e uma multiplicação do volume de dados a tratar. As ferramentas tradicionais da ciência forense demonstram-se, portanto, em muitos casos, insuficientes para lidar com esta nova realidade, tanto em termos de escala como de complexidade. As limitações de tempo, recursos humanos e capacidade computacional dificultam a extração de resultados eficazes. Neste contexto, a IA representa uma possível solução para alguns destes obstáculos.⁴⁴

Fala-se na tecnologia e IA como o próximo passo lógico na evolução humana com base na ideia de que está é capaz de tomar as suas decisões objetivamente, livre das limitações humanas que são a subjetividade, intuição e limitações cognitivas. No entanto, embora a IA possa significar otimizar processos, reduzir a carga de trabalho humano e revelar correlações invisíveis ao olhar analítico tradicional, não podemos ignorar os riscos e implicações sociais do seu uso, quando em causa pode estar, no limite e no contexto português, a privação da liberdade.

Não querendo, contudo, adiantar-nos na discussão ética que circunda este estudo, cabe-nos refletir sobre a realidade (já) atual do uso de *softwares* na investigação criminal. A IA já começa a ser largamente utilizada nos EUA, e em alguns países da Europa, na forma de instrumentos de “predictive policing”, fazendo uso das redes sociais e *softwares* de reconhecimento facial, assim como na forma de “automated” ou “digital evidence”⁴⁵.

Raffaele Olivieri, na sua tese de doutoramento, publicada em 2016⁴⁶, analisou um número elevado de casos reais do seu dia-a-dia como agente do laboratório forense de uma das forças policiais da Itália, com o objetivo de formular novas técnicas que pudessem ser utilizadas em laboratório. O autor foi capaz de, com o auxílio de técnicas

⁴⁴ Sónia Fidalgo, A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo, *op. cit.*; Yung-Fou Chen e Paul Kuei-chi Tseng, *The Boundary of Artificial Intelligence*, *op. cit.*; Dipo Dunsin, Mohamed C. Ghanem, Karim Ouazzane e Vassil Vassilev, *A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response*. *Forensic Science International: Digital Investigation* [online]. Vol. 48 (2024), 301675. Disponível em: <https://doi.org/10.1016/j.fsidi.2023.301675>.

⁴⁵ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, *op. cit.*.

⁴⁶ Raffaele Olivieri, *Digital Forensics meets Complexity Theory and Artificial Intelligence: Towards Automated Generation of Investigation Hypothesis*, tese de doutoramento em Engenharia e Ciências da Informação, Università degli Studi dell'Aquila, 2016. Orientadora: Prof.^a Stefania Costantini.

de *Computational Logic*⁴⁷ e codificação *ASP (Answer Set Programming)*⁴⁸, “identificar e tratar experimentalmente amostras que são representativas de classes significativas de investigações complexas, por analogia”⁴⁹.

Foi no seguimento desta investigação que, juntamente com Stefania Costantini e Giovanni De Gasperis, estudou a possibilidade de usar a IA (e as técnicas de *Computational Logic* e codificação *ASP* mencionadas) de forma a automatizar a análise de provas. O objetivo do estudo foi exatamente procurar comprovar que certas etapas/atividades da investigação criminal podem ser efetuadas por sistemas de IA. Sabendo que estas técnicas são raramente aplicadas na ciência forense e análise de provas, os autores procuraram estudar a sua aplicabilidade em futuros desenvolvimentos, avançando o estado da arte. Este estudo⁵⁰ foi posteriormente publicado em 2019 e pode resumir-se nas seguintes suposições:

1. Uma grande variedade de casos reais é passível de ser mapeada para problemas computacionais, uma vez que as atividades investigativas modernas são compostas por etapas práticas bem estabelecidas, tais como a reconstrução da cena do crime, a verificação de álibis e a análise de grandes volumes de dados provenientes de ficheiros digitais, registos de chamadas telefónicas e de *smartphones*, ou seja, seguem uma estrutura conhecida e previsível. A informação investigativa disponível pode, nesta perspetiva, ser tratada através de soluções algorítmicas cuja correção é apta a ser formalmente comprovada;
2. Nem todos os casos podem ser reduzidos a estes modelos de problemas, mas, quando aplicável, as formulações *ASP* são capazes de gerar todos os cenários possíveis compatíveis com os dados e restrições do caso, o que faz com que esta abordagem possa ser de grande utilidade, uma vez que o perito humano pode, por vezes, não considerar todas as possibilidades relevantes e

⁴⁷ A lógica computacional estuda como os princípios lógicos podem ser aplicados ao desenvolvimento de algoritmos e programas, usando linguagem formal para expressar declarações e regras que podem ser manipuladas automaticamente por computadores (John W. Lloyd, *Foundations of Logic Programming*. 2.^a ed. Berlin: Springer-Verlag, 1987, pp. 1-212)

⁴⁸ A *ASP* é um paradigma de programação declarativa assente em lógica, em que os problemas são representados por regras lógicas cuja solução corresponde aos *answer sets*, ou seja, interpretações que satisfazem o programa (Gerd Geberger, Nicola Leone e Simona Perri, *Answer Set Programming: An Introduction*. In: Pablo Barceló e Leonid Libkin (eds.), *Foundations of Artificial Intelligence*. Cambridge: Cambridge University Press, 2020, pp. 3-40.)

⁴⁹ No texto original, “identify and experimentally treat samples which are representative of significant classes of complex investigations by analogy”, *apud* Stefania Costantini, Giovanni De Gasperis e Raffaele Olivier, *Digital forensics and investigations meet artificial intelligence*, *op. cit.*

⁵⁰ Stefania Costantini, Giovanni De Gasperis e Raffaele Olivier, *Digital forensics and investigations meet artificial intelligence*, *op. cit.*

3. Na prática, espera-se que os investigadores sejam capazes de estabelecer analogias adequadas para interpretar os elementos de um caso e que façam uso das melhores técnicas e ferramentas sempre que estas estejam disponíveis. Assim, é razoável assumir que a metodologia proposta (que pretende apenas contribuir para a evolução das ferramentas atualmente existentes) possa ser utilizada.

No Capítulo 1 deste trabalho, foram apresentadas diversas definições de IA, com destaque para a sua aptidão para recolher e analisar dados do ambiente envolvente e, conseqüentemente, concretizar os objetivos previamente definidos pelos operadores humanos. Ainda assim, a IA distingue-se por um certo grau de autonomia, que lhe permite atuar independentemente. Esta autonomia é, muitas vezes, reforçada por mecanismos de aprendizagem automática (*machine learning*). Aplicando esta lógica ao contexto da análise da prova, é possível antever diversas vantagens na integração da IA nos processos forenses, nomeadamente: a) a redução do volume de dados a ser analisado manualmente pelos peritos; b) a identificação de correlações ou padrões que, pela sua complexidade ou escala, poderiam escapar à observação humana; c) a aplicação de métodos mais robustos de preservação da prova ao longo da investigação; e d) a minimização do risco de erro nas etapas de aquisição, conservação, análise e interpretação da prova⁵¹.

Apesar destas promessas, a realidade da aplicação da inteligência artificial nos contextos forenses revela-se mais complexa. É fundamental compreender de que forma estas tecnologias estão, de facto, a ser utilizadas na prática, e até que ponto estão a transformar o trabalho dos peritos humanos.

Yung-Fou Chen e Paul Kuei-chi Tseng publicaram, em 2023, o artigo científico “The Boundary of Artificial Intelligence in Forensic Science”, no qual reuniram de forma sumária e através da revisão teórica de vários autores, a realidade atual da IA nas ciências forenses, começando pela antropologia forense. Um dos contributos mais promissores da IA para a última prende-se com a possibilidade de padronizar imagens radiográficas e medições realizadas após a morte, facilitando a sua utilização em sistemas de aprendizagem automática. No entanto, a aplicação da IA neste domínio continua a levantar várias questões e dificuldades práticas, sobretudo quando o objetivo é

⁵¹ Sónia Fidalgo, A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo, *op. cit.*; Yung-Fou Chen e Paul Kuei-chi Tseng, *The Boundary of Artificial Intelligence in Forensic Science. op. cit.*; Dipo Dunsin, Mohamed C. Ghanem, Karim Ouazzane e Vassil Vassilev, *A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. op. cit.*

prever características como o sexo, a idade ou a ancestralidade de um indivíduo com base em restos mortais. Um dos maiores desafios diz precisamente respeito à recolha de dados adequados. Para que os algoritmos aprendam de forma eficaz, é necessário dispor de grandes amostras de restos esqueléticos de pessoas cuja identidade seja conhecida — uma tarefa que, por razões éticas, legais e logísticas, se revela particularmente complexa. Assim, muitos dos estudos existentes recorrem a dados recolhidos em pessoas vivas, normalmente com critérios de exclusão muito restritivos. Isso significa que situações mais complexas, como ossos alterados por trauma, cirurgias ou malformações, são muitas vezes deixadas de fora, o que limita a sua aplicabilidade real⁵².

A escassez de dados representativos e a dificuldade em considerar todas as variáveis que intervêm após a morte continuam, portanto, a ser o maior obstáculo. Ainda assim, noutras áreas, a IA tem demonstrado resultados encorajadores. Um exemplo é a odontologia forense, onde a tecnologia tem sido utilizada de forma experimental para apoiar processos de identificação. Nestes casos, tem-se recorrido à comparação entre radiografias dentárias (ortopantomografias) tiradas antes e depois da morte, o que tem permitido identificar, com algum sucesso, restos cadavéricos⁵³.

Também a patologia forense tem beneficiado da utilização de modelos computacionais capazes de reconhecerem padrões em imagens médicas relevantes, como exames radiológicos *post-mortem*, relatórios de autópsia ou análises microscópicas. No entanto, estas abordagens continuam a enfrentar vários entraves, como mudanças que ocorrem nos corpos após a morte, as diferenças nos procedimentos legais entre países e a diminuição do número de autópsias realizadas, que dificultam a criação de bases de dados consistentes e comparáveis^{54,55}.

Noutras áreas, como os laboratórios forenses, a IA tem vindo a ser utilizada com mais naturalidade, especialmente em tarefas como a extração e purificação de ADN. Organizações internacionais⁵⁶ têm emitido recomendações para orientar o desenvolvimento de programas informáticos que aplicam modelos probabilísticos à análise genética. Mesmo assim, a IA é, neste contexto, entendida como um apoio ao

⁵² Yung-Fou Chen e Paul Kuei-chi Tseng, *The Boundary of Artificial Intelligence in Forensic Science. op. cit.*.

⁵³ *Idem.*

⁵⁴ Além disso, importa reconhecer que a interpretação de dados forenses continua, em grande parte, dependente do olhar humano, o que pode introduzir subjetividade — um fator que levanta preocupações quando se pretende integrar a IA de forma ética e responsável.

⁵⁵ *Idem.*

⁵⁶ Grupo de Trabalho Científico sobre Métodos de Análise de ADN e a Sociedade Internacional de Genética Forense

trabalho dos especialistas humanos e não como um substituto. O seu papel é, para já, o de reforçar a eficiência, a precisão e a fiabilidade dos processos forenses⁵⁷.

Depois de tudo isto, importa ressaltar que nem todos os autores desta área procuram investigar e promover a parceria Humano-IA. Autores como Anabela Miranda Rodrigues, tomam uma posição mais defensiva quanto ao uso da IA na investigação criminal e, consequentemente, na justiça. Na sua posição, a investigação criminal, por natureza, representa um conflito entre a perseguição penal e os direitos fundamentais. Acrescentemos a este conflito a IA, cuja evolução é difícil de quantificar, e deixamos de falar somente de métodos de análise de prova mais sofisticados capazes de gerar todos os cenários possíveis, e passamos também a considerar dados gerados automaticamente, sem intervenção humana⁵⁸.

2.2 IA no processo penal, direito e justiça

A aplicabilidade da IA em vários níveis do sistema de justiça tem vindo a ser consistentemente estudada, estando já em uso em alguns deles, desde o auxílio à decisão judicial até à comparação entre a legislação vigente e a jurisprudência em casos semelhantes, possibilitando análises comparativas, a determinação concreta da pena, a avaliação do estado de inimputabilidade ou de imputabilidade reduzida, decisões sobre medidas de coação processual e, até mesmo, sobre a determinação da responsabilidade criminal e da sanção respetiva.⁵⁹ Um dos principais campos de atuação da IA é a justiça preditiva, que consiste no uso de sistemas computacionais para prever o resultado de litígios, a partir da análise de dados sobre as pessoas envolvidas e os seus históricos, com o intuito de estabelecer correlações e antecipar a sua perigosidade.⁶⁰

Contudo, é essencial refletir sobre as limitações destas tecnologias: como podem os sistemas de IA fundamentar os factos considerados provados ou não provados, quando a sua análise depende de critérios altamente subjetivos? Ainda que os algoritmos

⁵⁷ *Idem*.

⁵⁸ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, op. cit..

⁵⁹ André Lamas Leite, Prevenção policial e inteligência artificial no “Direito Penal da (pós-) modernidade”. Revista LEX de Criminologia & Vitimologia [online]. Vol. 3, n.º 8 (2023). Disponível em: <https://repositorio-aberto.up.pt/handle/10216/152412>.

⁶⁰ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, op. cit..

possam ser programados para reconhecerem esses elementos, seria tal programação capaz de captar a sua complexidade e *nuance*⁶¹.

Esta questão remete para um princípio básico da IA: se o *input* determina o *output*, o resultado final dependerá não só dos pressupostos iniciais que alimentaram o sistema, mas também da forma como este evoluiu ao longo do tempo. No contexto da determinação da responsabilidade penal e da determinação da medida concreta da pena, isto implica reconhecer que os sistemas podem refletir viés ou limitações embutidas desde o seu início⁶². Além disso, o recurso à prova algorítmica, com a sua inerente opacidade, coloca em risco o princípio da igualdade de armas no processo penal⁶³.

No processo criminal, a lógica da causalidade orienta as decisões, tradicionalmente baseadas em dois modelos: o narrativo, centrado na história dos fatos, e o argumentativo, focado nas provas. A objetividade trazida pelos algoritmos pode ser vista como um benefício, ao afastar subjetividades e preconceitos humanos que alimentam a arbitrariedade. Retirar ao juiz o poder da decisão arbitrária pode, em muitos aspetos, ser positivo. Contudo, existe o risco de que essa objetividade excessiva elimine também a discricionariedade, que é fundamental para que a decisão judicial incorpore intuição e valorações pessoais. Sobretudo no âmbito penal, a decisão judicial envolve não apenas o rigor técnico, mas também um elemento humano que confere sensibilidade e humanidade à justiça⁶⁴. Face ao que foi dito e à realidade atual dos sistemas de IA, parece improvável que o juiz possa ser inteiramente substituído pela máquina. A ligação entre liberdade e culpa, com as suas inúmeras combinações possíveis, ainda está fora do alcance das tecnologias existentes, sobretudo quando se exige um grau de fundamentação crítica⁶⁵.

Diante deste cenário, é necessário refletir sobre os riscos da previsibilidade trazida pela IA para a justiça penal. A discussão já não é sobre ser a favor ou contra a IA, mas sobre como garantir que o papel humano no processo decisório é preservado. Os sistemas de IA apenas indicam a probabilidade de que um juiz tome uma decisão semelhante a outras já adotadas, sem fundamentar o raciocínio jurídico nem compreender as relações de imputação objetiva que estão na base da decisão. Neste

⁶¹ André Lamas Leite, *Prevenção policial e inteligência artificial no "Direito Penal da (pós-) modernidade"*, *op. cit.*.

⁶² *Idem.*

⁶³ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, *op. cit.*.

⁶⁴ *Idem.*

⁶⁵ André Lamas Leite, *Prevenção policial e inteligência artificial no "Direito Penal da (pós-) modernidade"*, *op. cit.*.

âmbito, os autores criticam o facto de estes sistemas se limitarem a reproduzir correlações entre palavras e decisões anteriores, sem captar a complexidade do raciocínio jurídico ou explicar retroativamente a atuação do juiz⁶⁶.

Sob uma perspetiva epistemológica, é fundamental justificar a permanência do ser humano na tomada de decisões penais, se os resultados gerados pela IA parecem mais objetivos e confiáveis. A justificação está clara no fato de o juiz não decidir apenas sobre dados técnicos ou científicos, mas sobre a responsabilidade criminal individual, o que envolve o julgamento ético-social. A função judicial implica compreender o caso concreto e as características da pessoa julgada, um elemento essencial para garantir a prudência e a aceitação social da decisão. Aliás, em Direito Penal, não se julga a pessoa em si mesmo considerada, por absoluta falta de legitimidade deste ramo do Direito para tal e visto que esse julgamento conduziria a uma inaceitável instrumentalização da pessoa humana, mas julgam-se sim os atos e omissões por ele praticados, *rectius*, que lhe possam ser imputados em termos de ilicitude e de culpa, percorrendo e preenchendo todos os escalões do conceito material de crime (conduta humana, tipicidade, ilicitude, culpa e, para alguns autores, punibilidade). A discricionariedade não é apenas um atributo do juiz, mas uma dimensão que permite a adequação da pena e a sua responsabilidade, algo que um sistema algorítmico automático não pode substituir⁶⁷.

Outro aspeto preocupante é a submissão do juiz à máquina, que pode ocorrer devido à tendência humana de confiar excessivamente em procedimentos computacionais. Este fenómeno, conhecido como viés automático (*automation bias*), ocorre quando o decisor humano não procura informações contrárias à solução gerada pelo algoritmo, colocando em risco a experiência profissional e a discricionariedade do juiz. Adicionalmente, condenações baseadas exclusivamente em dados algorítmicos contradizem fundamentos centenarios do Direito Penal, que distinguem o facto praticado das motivações e do comportamento do indivíduo⁶⁸. Este ramo do Direito valoriza o contexto pessoal para garantir uma punição justa e a fim de evitar preconceitos. Contudo,

⁶⁶ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, op. cit..

⁶⁷ Anabela Miranda Rodrigues, A questão da pena e a decisão do juiz – entre a dogmática e o algoritmo. In: Anabela Miranda Rodrigues (coord.) – *A Inteligência Artificial no Direito Penal*. Coimbra: Edições Almedina, 2022, pp. 219-244; Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a Justiça Preditiva entre a Americanização e a Europeização*, op. cit..

⁶⁸ Por consequência, o avanço do cálculo preditivo representa uma mudança significativa no Direito Penal, trazendo um determinismo que restringe a flexibilidade do Direito. A transformação do discurso jurídico da escrita alfabética para a escrita numérica modifica o seu sentido e processo, deslocando a causalidade jurídica para uma simples correlação matemática. Essa normatividade preditiva, distinta da normatividade jurídica tradicional, não estabelece ligações lógicas entre proposições, mas baseia-se em correlações puramente matemáticas.

a justiça preditiva, ao basear-se em perfis algorítmicos, elimina esta distinção e substitui a discricionariedade pela determinação rígida, ignorando o contexto vivido pelo autor do crime, que não pode ser adequadamente traduzido em algoritmos⁶⁹.

No domínio da prova digital, a utilização da IA amplia os meios de investigação, mas levanta questões sobre os direitos fundamentais. A complexidade e a opacidade destes sistemas podem comprometer o direito de defesa, uma vez que a fiabilidade da prova depende da exatidão dos meios tecnológicos usados. É legítimo questionar se é possível ter a certeza da correção dos dados obtidos exclusivamente por IA e se existe a possibilidade de os contestar. Esta opacidade assemelha-se ao problema das testemunhas anónimas, cuja admissibilidade depende da aplicação rigorosa de regras para proteger o arguido. Por isso, é imprescindível questionar se o direito de defesa está verdadeiramente salvaguardado quando estas técnicas são utilizadas na obtenção de prova⁷⁰.

Para que a defesa seja efetiva, o arguido deve ter a oportunidade real e eficaz de contestar a prova apresentada. No caso da IA, essa possibilidade fica claramente prejudicada, pois o arguido só poderá exercer o seu direito se tiver acesso a informações técnicas. Assim, os sistemas de IA utilizados na prova digital precisam de ser explicáveis e transparentes, garantindo que os seus resultados sejam compreensíveis para todos os intervenientes no processo, com total clareza sobre os dados de base e o modo como as conclusões foram alcançadas⁷¹.

3. Modelos de colaboração Humano-IA: o que existe?

A utilização da IA no sistema de justiça penal introduziu uma nova dimensão — a da previsão —, permitindo, em teoria, que a intervenção penal ocorra antes da concretização de um crime, com o objetivo de o evitar. No âmbito específico da investigação policial, debate-se o policiamento preditivo.

O *predictive policing* (também referido como justiça preditiva ou policiamento preditivo) pode ser entendido como o processo de recolha e análise de dados provenientes de diferentes fontes, com o propósito de prever comportamentos futuros e, assim, possibilitar a aplicação de estratégias que permitam antecipar, prevenir e

⁶⁹ Anabela Miranda Rodrigues, A questão da pena e a decisão do juiz – entre a dogmática e o algoritmo, *op. cit.*; Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a Justiça Preditiva entre a Americanização e a Europeização*, *op. cit.*.

⁷⁰ Sónia Fidalgo, A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo, *op. cit.*.

⁷¹ *Idem*.

responder de forma mais eficaz a tais comportamentos⁷². Trata-se, portanto, da utilização de sistemas de IA que, com base na recolha de grandes volumes de dados, procuram antecipar a ocorrência de crimes, sendo essa informação utilizada pelas forças policiais e demais entidades competentes⁷³.

No contexto europeu, certas práticas de policiamento preditivo enquadram-se no âmbito do novo Regulamento do Parlamento Europeu e do Conselho sobre regras harmonizadas relativas à Inteligência Artificial. Em 2024, o Parlamento Europeu aprovou este regulamento, sem, contudo, apresentar uma definição formal de policiamento preditivo^{74,75}.

Entre os países europeus, a França destaca-se pelo dinamismo do debate em torno da justiça preditiva. Após a aprovação da lei *République numérique*, que visava reforçar a transparência no funcionamento dos tribunais, a administração pública francesa foi obrigada a disponibilizar *online* todas as decisões judiciais proferidas no país. Esta medida originou um vasto repositório de dados judiciais, rapidamente explorado por *startups* francesas de *legaltech*⁷⁶.

Em Portugal, embora o país participe em diversos projetos europeus cofinanciados pela UE para a aplicação da IA na atividade policial, nomeadamente através da Polícia Judiciária, não existem registos da utilização efetiva de sistemas de policiamento preditivo. Já noutros países europeus, estes mecanismos são abertamente utilizados para fins de investigação criminal⁷⁷.

Na Alemanha, por exemplo, um destes sistemas esteve no centro de uma decisão do Tribunal Constitucional, em fevereiro de 2023. O *software* em questão, *Gotham*, desenvolvido pela *Palantir Technologies*, foi adquirido em 2017 pelo Estado de Hesse,

⁷² Fernanda Silva Lobato, *Uso de softwares com função analítica preditiva aplicados à investigação criminal e atividade de inteligência: uma análise sobre o conflito de normas relativas ao direito constitucional à privacidade e à segurança pública*, op. cit..

⁷³ Ana Pais, *Investigação policial e Inteligência Artificial: o policiamento preditivo e os atuais desafios ao direito*. Em especial, o caso *HessenDATA* e a relevância da decisão do *Bundesverfassungsgericht* de 16 de fevereiro de 2023. In: Anabela Miranda Rodrigues (coord.) – *A Inteligência Artificial no Direito Penal*. Vol. III. Coimbra: Edições Almedina, 2022, pp. 167-188.

⁷⁴ Contudo, determinadas práticas de policiamento preditivo enquadram-se claramente entre as aplicações de IA proibidas pelo referido Regulamento, enquanto outras, ainda que abrangidas pelo conceito, inserem-se inequivocamente na categoria de sistemas de IA de alto risco.

⁷⁵ *Idem*.

⁷⁶ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, op. cit..

⁷⁷ Ana Pais, *Investigação policial e Inteligência Artificial: o policiamento preditivo e os atuais desafios ao direito*. Em especial, o caso *HessenDATA* e a relevância da decisão do *Bundesverfassungsgericht* de 16 de fevereiro de 2023, op. cit..

onde passou a ser designado *HessenDATA* (posteriormente também utilizado em Hamburgo)⁷⁸. Este sistema permitia à polícia, em casos autorizados, processar informação pessoal armazenada, através de análise automatizada de dados, tanto para prevenir crimes graves como para proteger certos interesses jurídicos. Este *software* tem a capacidade de cruzar e agregar grandes quantidades de informação, ligando dados de bases policiais a conteúdos provenientes de meios de comunicação social, redes sociais e plataformas de autoridades oficiais. Apesar de os Estados envolvidos terem tentado dissociar o programa de práticas de policiamento preditivo, o Tribunal concluiu que os dados recolhidos não só serviam para efeitos de investigação criminal como também possibilitavam a criação de perfis de suspeitos⁷⁹.

Embora presente no espaço europeu, com o policiamento preditivo, a IA encontra-se mais disseminada em países de tradição do *common law*, como os Estados Unidos e o Reino Unido, sobretudo na fase de execução das penas, incluindo decisões sobre liberdade condicional, caução e *sentencing*. Nos últimos anos, os EUA têm assistido a um crescimento acelerado do uso de ferramentas algorítmicas de avaliação de risco. Estima-se que mais de sessenta destes instrumentos estejam atualmente em uso, abrangendo todas as fases do sistema de justiça penal, e já se estendendo ao Canadá, Austrália e Reino Unido⁸⁰. O Estado da Virgínia foi pioneiro na criação de instrumentos para aplicação na fase de *sentencing*, sendo o “Level of Service Inventory – Revised” (*LSI-R*) e o “Correctional Offender Management Profiling for Alternative Sanction” (*COMPAS*) os mais conhecidos⁸¹.

O *COMPAS* tem sido alvo de críticas significativas⁸², nomeadamente por parte da organização *ProPublica*, que apontou para a existência de discriminação racial, falta de

⁷⁸ A plataforma terá sido empregue em aproximadamente 12.000 casos como medida preventiva contra crimes graves. O processo teve início após uma queixa da Sociedade Alemã de Direitos Cíveis, que alegou que o *software* utilizou de forma ilegítima dados de indivíduos inocentes para gerar suspeitas, nem sempre devidamente fundamentadas.

⁷⁹ *Idem*.

⁸⁰ Anabela Miranda Rodrigues, A questão da pena e a decisão do juiz – entre a dogmática e o algoritmo, *op. cit.*.

⁸¹ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, *op. cit.*.

⁸² Em 2013, Eric Loomis foi acusado, em Wisconsin, por cinco crimes. No acordo de *plea bargaining*, confessou três e foi julgado pelos dois restantes. Antes da sentença, foi elaborado um relatório prévio que incluía a avaliação do sistema COMPAS, o qual classificou Loomis como de “alto risco de reincidência” e “alto risco para a comunidade”. Com base nesses resultados, foi-lhe aplicada a pena máxima. Loomis recorreu, alegando que: (1) o uso do COMPAS violava o *due process*, pois o seu funcionamento era sigiloso; (2) foi negado o direito a uma avaliação individualizada, já que o COMPAS foi concebido para análises de grupos; e (3) a ferramenta utilizava indevidamente o “género” como variável na avaliação de risco.

transparência e eficácia preditiva duvidosa⁸³. Desenvolvido pela *Northpointe*, o *COMPAS* avalia risco e necessidades: a escala de risco procura prever a probabilidade de reincidência, enquanto a escala de necessidades identifica áreas de intervenção. O questionário associado inclui elementos estáticos, como o registo criminal, e dinâmicos, como convicções pessoais, níveis de confiança e perceções sobre o que é “certo” ou “errado”⁸⁴.

Ainda nos EUA, em 2006, foi criada a “Intelligence Advanced Research Projects Activity” (*IARPA*), uma agência responsável por promover e financiar a investigação para superar desafios estratégicos dos órgãos de inteligência, entre os quais se inclui o policiamento preditivo. A Polícia de Los Angeles (LAPD) é considerada uma das pioneiras na aplicação de tecnologias avançadas de policiamento preditivo, com três projetos ativos, incluindo um dedicado à análise de redes sociais para investigações sobre gangues e grupos organizados. Já em Washington, a Polícia Metropolitana conta com um departamento especializado na recuperação de armas que utiliza *software* de mapeamento de dados⁸⁵.

No Reino Unido, destaca-se o desenvolvimento do “Harm Assessment Risk Tool” (*HART*), criado em colaboração com a Universidade de Cambridge, cujo objetivo é avaliar o risco de reincidência de detidos e apoiar decisões sobre programas de reabilitação. No entanto, a utilização deste sistema tem gerado críticas relacionadas com questões de privacidade, proibição de perfis discriminatórios, decisões automatizadas, discriminação algorítmica e garantia de *fairness* no sistema penal⁸⁶.

O impacto da IA no sistema de justiça não se limita ao policiamento preditivo ou ao *sentencing*. A tecnologia tem vindo a ser aplicada também no contexto prisional, através de sistemas de vigilância avançados. Alguns estabelecimentos já se transformaram em “prisões inteligentes”, sobretudo na Ásia. Em Singapura, existe uma prisão totalmente automatizada, operada por IA e robôs, sem guardas humanos. Na China, foi implementado um sistema de vigilância inteligente para monitorização constante dos reclusos, incluindo no interior das celas. Em Hong Kong, câmaras com

⁸³ *Idem*.

⁸⁴ Rui Caria, O caso *State v. Loomis* – a pessoa e a máquina na decisão judicial. In: Anabela Miranda Rodrigues (coord.) – *A Inteligência Artificial no Direito Penal*. Coimbra: Edições Almedina, 2022. P. 245-265.

⁸⁵ Fernanda Silva Lobato, *Uso de softwares com função analítica preditiva aplicados à investigação criminal e atividade de inteligência: uma análise sobre o conflito de normas relativas ao direito constitucional à privacidade e à segurança pública*, op. cit..

⁸⁶ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, op. cit..

análise de vídeo baseada em IA identificam comportamentos incomuns e alertam as autoridades. Na Coreia do Sul, robôs patrulham prisões para prevenirem violência e suicídios⁸⁷.

Nos EUA, algumas prisões em Nova Iorque e no Alabama utilizam sistemas de monitorização de chamadas telefónicas de reclusos, com reconhecimento de voz, análise semântica e *machine learning* para identificarem termos associados a comportamentos suspeitos. Já no Reino Unido, em Liverpool, uma prisão utiliza câmaras monitorizadas por IA para detetar ações potencialmente perigosas⁸⁸.

O uso da IA no sistema de justiça penal representa uma mudança significativa na forma como as instituições lidam com a criminalidade. Embora estas tecnologias ofereçam oportunidades para maior eficiência e prevenção, levantam igualmente desafios éticos, jurídicos e sociais de grande relevância, como a proteção da privacidade, a prevenção de discriminação e a garantia de transparência. O equilíbrio entre inovação e salvaguarda dos direitos fundamentais vai determinar o futuro destes sistemas.

4. Desafios e questões éticas

Já hoje é possível que as pessoas venham a estar cada vez mais sujeitas a decisões tomadas, se não integralmente por IA, pelo menos com o seu apoio direto ou indireto. A UE tem vindo a manifestar uma atenção especial a este fenómeno. O Livro Branco sobre a Inteligência Artificial⁸⁹ dedica algum espaço a este tema, mencionando expressamente direitos como a liberdade de expressão, a dignidade, a não-discriminação por motivos de sexo, origem racial ou religião, idade, orientação sexual e identidade de género, bem como o direito a recurso judicial, à proteção de dados pessoais e à privacidade⁹⁰.

Fora do espaço europeu, nos EUA, por exemplo, discute-se sobretudo a fraca representatividade dos dados utilizados pelos sistemas de avaliação de risco. Muitos dos elementos usados para prever comportamentos violentos têm pouco ou nenhum valor

⁸⁷ Anabela Miranda Rodrigues e Sónia Fidalgo, *Pena de Prisão e Inteligência Artificial – o que esperar de uma aliança (im)provável*. In: Anabela Miranda Rodrigues (coord.) – *A Inteligência Artificial no Direito Penal*. Vol. III. Coimbra: Edições Almedina, 2022, pp. 263-285.

⁸⁸ *Idem*.

⁸⁹ *Livro Branco sobre a Inteligência Artificial — Uma abordagem europeia virada para a excelência e a confiança*, COM (2020) 65 final, Bruxelas, 19-02-2020. Disponível em https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_pt?file_name=commission-white-paper-artificial-intelligence-feb2020_pt.pdf.

⁹⁰ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, *op. cit.*.

criminológico, funcionando antes como indicadores de vulnerabilidade social. O efeito prático é o reforço de desigualdades já existentes no sistema judicial norte-americano. A inclusão de certas variáveis pode ainda conduzir a que o comportamento passado de uma pessoa, por estar associado a um grupo social, determine o seu futuro, pois um *software*, ao contrário de um juiz, não consegue ponderar estas variáveis de acordo com o seu contexto e o contexto de vida do indivíduo⁹¹.

Convém recordar que o preconceito e a discriminação não são fenómenos exclusivos da tecnologia: são riscos presentes em qualquer atividade económico-social e, por conseguinte, também nas decisões humanas. No entanto, no caso da IA, estes enviesamentos adquirem uma amplitude potencialmente maior, afetando um maior número de pessoas e sem o “filtro” do controlo social que regula o comportamento humano⁹².

Anabela Rodrigues desenvolve a temática em vários dos seus artigos, citando Yuval Noah Harari, que sustenta não haver “razão para assumirmos que os algoritmos não poderão ter um desempenho ético superior ao humano”. Para a autora, se um sistema for programado para ignorar fatores como sexo biológico, identidade de género ou origem racial, assim o fará, dado que “os computadores não têm subconsciente”. Poder-se-ia, então, imaginar como hipótese a introdução de dados adicionais — por exemplo, intuições e valorações pessoais — convertidos em *inputs* para processamento automático, de forma a colmatar estas limitações. Todavia, como estas informações não existem em bases de dados, tal solução não se revela tecnicamente exequível⁹³.

Mesmo com avanços significativos, o *machine learning* permanece vulnerável. A prova obtida através destas técnicas é frágil, sobretudo porque a eficácia de muitos sistemas de IA depende de vastos volumes de dados. Se estes forem enviesados, desequilibrados ou pouco inclusivos, a capacidade de generalização do sistema ficará comprometida, originando decisões “erradas”. Acresce que os sistemas aplicados à ciência forense digital são igualmente suscetíveis a erros e a ataques, incluindo *inputs* contraditórios ou envenenamento de dados⁹⁴.

Um dos pontos mais delicados reside na interação entre humanos e máquinas. Embora estas ferramentas possam auxiliar juízes, aumentando a eficácia e reduzindo a

⁹¹ *Idem.*

⁹² *Idem.*

⁹³ *Idem.*

⁹⁴ Sónia Fidalgo, A utilização de inteligência artificial no âmbito da prova digital – direitos fundamentais (ainda mais) em perigo, *op. cit.*

subjetividade, a delegação excessiva da responsabilidade de decisão aos algoritmos levanta questões éticas sérias. Não se trata apenas de avaliar a credibilidade ou eficiência técnica destes instrumentos, mas de refletir sobre se decisões de enorme impacto, como as judiciais, devem ser tomadas exclusivamente com base na rapidez e na eficácia do processo. Alguns autores chegam a referir-se a um “genocídio humano” para descrever a delegação da responsabilidade decisória em máquinas. Mas será correto afirmar que estamos a abdicar das nossas decisões, quando os sistemas são concebidos por nós?⁹⁵

É inegável que esta evolução é irreversível: a IA já está presente e continuará a evoluir. Do ponto de vista técnico, é possível imaginar um sistema com capacidade de agência moral. No entanto, a possibilidade não implica a necessidade. Todo o sistema de IA é um produto do *design* humano; por conseguinte, a decisão de dotá-lo de moralidade será também nossa e, como tal, pode ser evitada. Parafraseando Anabela Miranda Rodrigues⁹⁶, talvez a opção mais ética seja precisamente escolher não o fazer.

5. A integração ótima: reflexões e discussão

A presença da IA no sistema de justiça criminal é já uma realidade incontornável, como temos vindo a dizer. A questão que se coloca não é se esta tecnologia será utilizada, mas como será integrada de forma a reforçar a eficácia do sistema sem comprometer as garantias fundamentais. Tal integração deve, acima de tudo, respeitar a natureza própria do processo penal, onde a verdade nunca se estabelece como uma certeza científica absoluta, mas como um juízo construído a partir da prova produzida e apreciada segundo o princípio da livre convicção. No julgamento penal, a dúvida não é uma falha a eliminar; é um elemento estruturante, que protege contra a precipitação e o erro irreversível. E mais: a dúvida tem um dado resultado previsto para o processo criminal. O princípio do *in dubio pro reo* trata exatamente de uma dúvida insanável do julgador que, após a produção de toda a prova, não consegue afirmar, com o grau de certeza exigível (para além de toda a dúvida razoável: *beyond any reasonable doubt*), que o arguido cometeu o crime, pelo que tem de existir um mecanismo que, quase de modo automático, permita ultrapassar a situação de dúvida que, *in casu*, terá sempre de ser valorada a favor do arguido, uma vez que este é titular da presunção de inocência que se retira do art. 32.º, n.º 2, da nossa Constituição. Onde, é essencial que os programas de IA tenham apreendido este princípio estruturante de todo o processo penal

⁹⁵ Anabela Miranda Rodrigues, *Inteligência Artificial no Direito Penal: a justiça preditiva entre a americanização e a europeização*, op. cit..

⁹⁶ *Idem*.

e que, depois de identificarem uma dúvida, a caracterizem como ultrapassável ou não e decidam em conformidade. Neste momento da evolução da técnica, saber se uma dúvida, no espírito do julgador, é passível de ser ultrapassada ou não, por relação entre todos os meios de prova produzidos ou examinados em audiência de discussão e julgamento (art. 355.º do Código de Processo Penal) e aqueles que são preexistentes, ou seja, a prova pré-constituída, parece ainda longe de ser uma realidade. No entanto, tendo em conta todos os desenvolvimentos até hoje, podemos concluir que é apenas uma questão de tempo até que aquilo que se julgava impossível se torne realidade.

A modernização do processo penal é inevitável. A realidade digital em que vivemos exige ferramentas capazes de lidar com volumes de dados que ultrapassam, em muito, a capacidade de processamento humano. Não se pode, portanto, rejeitar a tecnologia, sob pena de se condenar o sistema judicial à obsolescência. No entanto, integrar a IA não significa ceder-lhe o papel central da decisão, mas utilizá-la como um prolongamento das capacidades humanas, um instrumento que amplia a análise e a investigação.

A integração ótima da IA deve assentar em três pilares: precaução, proporcionalidade e transparência. A precaução impõe que qualquer aplicação desta tecnologia seja precedida de uma avaliação rigorosa dos riscos, sobretudo no que respeita à preservação dos direitos fundamentais. A proporcionalidade exige que a intervenção tecnológica seja sempre adequada à finalidade pretendida, evitando a intrusão desnecessária na esfera privada. A transparência, por sua vez, implica que os sistemas sejam compreensíveis para todos os intervenientes, permitindo que os seus resultados sejam explicados e, quando necessário, contestados.

Num cenário ideal, a IA atuaria como parceira de investigação, assumindo funções repetitivas, de triagem e de análise técnica de grandes volumes de dados. Poderia, por exemplo, cruzar registos telefónicos, metadados e imagens digitais para identificar padrões relevantes, deixando ao perito humano a tarefa de interpretar o seu significado probatório. No campo forense, poderia auxiliar na preservação da cadeia de custódia, detetar anomalias ou incongruências na prova e reduzir o tempo necessário para a análise de elementos técnicos complexos. Crucialmente, em nenhuma destas etapas a máquina substituiria o juízo humano sobre a relevância, fiabilidade e significado da prova.

O risco mais evidente desta transformação reside na tentação de delegar a decisão às máquinas. O fenómeno conhecido como *automation bias*, que já

mencionámos, revela que, perante uma resposta tecnológica aparentemente objetiva, o decisor humano tende a abdicar da sua própria avaliação crítica⁹⁷

A justiça criminal não pode tornar-se refém de modelos preditivos que, por mais sofisticados que sejam, apenas reproduzem padrões encontrados em dados passados. Ao fazê-lo, arriscar-se-ia a cristalizar desigualdades e a eliminar a flexibilidade necessária para julgar cada caso de forma individualizada. A lógica da previsão pode ser útil para compreender tendências, mas não para determinar culpas ou penas.

Uma integração equilibrada da IA requer, portanto, limites claros. É essencial que o controlo humano seja significativo e não meramente simbólico, que os sistemas sejam auditáveis por entidades independentes e que as partes no processo — acusação e defesa — tenham igual acesso à informação sobre o funcionamento e os resultados da tecnologia utilizada. Só assim se garante a igualdade de armas e se evita que a opacidade tecnológica se transforme em um obstáculo ao direito de defesa.

A melhor forma de olhar para a IA no processo penal é vê-la como um microscópio: uma ferramenta que permite observar melhor, mais fundo e com mais detalhe, mas que não nos diz, por si só, o que significa o que estamos a ver. A interpretação continua a caber ao investigador, ao perito e, em última instância, ao juiz.

Para que a integração da IA seja não apenas tecnicamente possível, mas eticamente aceitável, é necessário delimitar com clareza onde pode e deve ser utilizada, e onde não deve ultrapassar a sua função de apoio. Seguem-se, assim, algumas possíveis aplicações:

1. Análise forense digital: A IA pode acelerar a triagem de dispositivos eletrónicos, identificando ficheiros relevantes e ordenando-os por pertinência. No entanto, o conteúdo deve ser sempre revisto por peritos humanos, de forma a contextualizar e validar a interpretação.
2. Preservação da prova: Algoritmos podem ajudar a monitorizar alterações nos ficheiros e registar automaticamente cada acesso, fortalecendo a cadeia de custódia. Aqui, o papel humano é de supervisão e verificação periódica.

⁹⁷ No processo penal, esta abdicção seria particularmente perigosa, pois a decisão judicial não é apenas um exercício técnico: é um ato de ponderação ético-social, que envolve a apreciação do caso concreto, das circunstâncias pessoais do arguido e das consequências da sanção criminal. O mesmo resulta do processo de determinação da medida da pena, partindo-se da moldura penal abstrata para a medida concreta da pena, passando pela moldura concreta (cf. artigos 40.º, 70.º e 71.º, todos do Código Penal).

3. Identificação de padrões em investigações complexas: A IA pode cruzar dados de diferentes fontes — registos policiais, redes sociais, transações financeiras — para identificar redes de contacto ou fluxos suspeitos. A interpretação, contudo, deve ser sempre humana, evitando conclusões baseadas apenas em correlação.
4. Limitação no policiamento preditivo: A utilização de IA para prever crimes deve ser restrita a contextos em que haja forte validação empírica e garantia de que não há discriminação estrutural. Qualquer decisão que afete direitos individuais (prisão, medidas de coação) deve basear-se em avaliação humana independente.
5. Exclusão de decisões penais automáticas: Determinação de culpabilidade, aplicação de penas ou avaliação de perigosidade não devem ser entregues à máquina. Estes juízos envolvem elementos morais e sociais que nenhum algoritmo consegue reproduzir de forma legítima.

No fim, a integração ótima da IA não será definida pelo grau de automação alcançado, mas pela capacidade de preservar o carácter humano da justiça enquanto se tira partido do potencial transformador da tecnologia.

6. Conclusão

A IA, no sistema de justiça criminal e forense, representa uma transformação profunda, que combina oportunidades inéditas de eficiência com desafios éticos e sociais. Ao longo desta dissertação, procurámos explorar não apenas o estado atual das tecnologias disponíveis, mas também a forma como estas se articulam com os processos humanos de decisão, responsabilidade e interpretação jurídicas.

Os sistemas de IA, desde o policiamento preditivo até à análise forense digital, oferecem vantagens na gestão de grandes volumes de dados e na identificação de padrões complexos que ultrapassam a capacidade humana. Ferramentas como o *COMPAS*, o *HART* ou os *softwares* utilizados em prisões inteligentes exemplificam esta potencialidade, permitindo intervenções mais rápidas, precisas e, em teoria, preventivas. A aplicação destas tecnologias pode aumentar a eficiência das investigações, reduzir erros técnicos e permitir uma melhor alocação de recursos humanos, libertando peritos e decisores de tarefas repetitivas e técnicas para que possam concentrar-se na interpretação e na ponderação ética dos casos.

No entanto, a presença da IA no sistema penal também evidencia riscos que não podem ser ignorados. A utilização de algoritmos para avaliar o risco, prever comportamentos ou orientar decisões de pena levanta questões fundamentais sobre privacidade, não-discriminação e transparência. Os enviesamentos nos dados, a possibilidade de reforço de desigualdades sociais e a tentação de delegar decisões morais a máquinas evidenciam que a tecnologia, por mais avançada que seja, nunca pode substituir o juízo humano. A experiência norte-americana com o *COMPAS* ou o caso do *software Gotham* na Alemanha demonstram que mesmo sistemas sofisticados podem perpetuar padrões de discriminação ou gerar falsas percepções de objetividade.

É, portanto, essencial que a IA seja encarada como parceira, e não como substituta, da decisão humana. A integração ótima implica um equilíbrio delicado: por um lado, aproveitar o potencial transformador da tecnologia para tornar o sistema mais eficaz e preciso; por outro, preservar o carácter humano do processo penal, garantindo que a ponderação ética, o contexto individual e a análise crítica permaneçam sob controlo humano. A IA deve atuar como um microscópio ou uma lupa que amplia a visão, sem ditar conclusões.

Três princípios orientadores emergem como fundamentais para qualquer implementação responsável: precaução, proporcionalidade e transparência. Aplicações concretas como a triagem de dados digitais, a monitorização da cadeia de custódia, ou a identificação de padrões em investigações complexas, exemplificam como a IA pode ser útil, desde que a interpretação final permaneça humana. Por outro lado, decisões sobre culpabilidade, imposição de penas ou avaliação de perigosidade não devem ser delegadas a algoritmos.

A análise aqui desenvolvida evidencia ainda uma dimensão mais ampla: a IA no sistema de justiça não é apenas uma questão técnica, mas sobretudo social, ética e política. A forma como estruturamos os sistemas de decisão, selecionamos os dados e definimos os limites da automação reflete escolhas de valor sobre justiça, equidade e direitos humanos. Nesse sentido, a investigação futura poderá explorar diversas frentes. Entre estas, destacam-se a avaliação comparativa de diferentes modelos de colaboração humano-IA em contextos penais, a análise da percepção social sobre decisões assistidas por IA, e o desenvolvimento de indicadores que permitam medir não apenas a eficácia técnica, mas também a justiça, a equidade e a aceitabilidade ética das intervenções. Outra área promissora é a investigação interdisciplinar, para definir *frameworks* robustos, inclusivos e adaptáveis a diferentes contextos legais.

Em última análise, esta dissertação sublinha que a presença da IA no sistema de justiça criminal é inevitável, mas não é determinista. Não se trata de abdicar da decisão humana, mas de construir uma parceria que potencia capacidades. O futuro da justiça humano-IA depende das escolhas que fizermos hoje sobre limites, supervisão, transparência e valores que queremos preservar. Esta é, talvez, a maior oportunidade (e responsabilidade) das sociedades contemporâneas: desenhar sistemas em que a tecnologia amplie a justiça, sem jamais a substituir.

Referências

Bibliografia citada

CARIA, Rui – O caso *State v. Loomis* – a pessoa e a máquina na decisão judicial. In: RODRIGUES, Anabela Miranda (coord.) – *A Inteligência Artificial no Direito Penal*. Coimbra: Edições Almedina, 2022, pp. 245-265.

CHEN, Yung-Fou; TSENG, Paul Kuei-chi – *The Boundary of Artificial Intelligence in Forensic Science*. *DIALOGO* [em linha]. Vol. 10, n.º 1 (2023), pp. 49–60. Disponível em: <https://doi.org/10.51917/dialogo.2023.10.1.5>

COSTANTINI, Stefania; DE GASPERIS, Giovanni; OLIVIER, Raffaele – *Digital forensics and investigations meet artificial intelligence*. *Annals of Mathematics and Artificial Intelligence*. Vol. 86, nr. 2, (2019), pp. 193-229. DOI: 10.1007/s10472-019-09632-y. Publicado em 24 de abril de 2019.

DUNSIN, Dipo; GHANEM, Mohamed C.; OUZZANE, Karim; VASSILEV, Vassil – *A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response*. *Forensic Science International: Digital Investigation* [online]. Vol. 48 (2024), 301675. Disponível em: <https://doi.org/10.1016/j.fsidi.2023.301675>.

FIDALGO, Sónia – *A utilização de inteligência artificial no âmbito da prova digital - direitos fundamentais (ainda mais) em perigo*. In: RODRIGUES, Anabela Miranda (coord.) – *A Inteligência Artificial no Direito Penal*. Coimbra: Edições Almedina, 2022, pp. 129-161.

GEBERGER, Gerd; LEONE, Nicola; PERRI, Simona – *Answer Set Programming: An Introduction*. In: BARCELÓ, Pablo; LIBKIN, Leonid (eds.) – *Foundations of Artificial Intelligence*. Cambridge: Cambridge University Press, 2020, pp. 3-40.

JADHAV, Ekta B.; SANKHLA, Mahipal Singh; KUMAR, Rajeev – *Artificial Intelligence: Advancing Automation in Forensic Science & Criminal Investigation* [online]. *Seybold Report*, 2020, vol. 15, pp. 2064-2075. Disponível em: https://www.researchgate.net/publication/343826071_Artificial_Intelligence_Advancing_Automation_in_Forensic_Science_Criminal_Investigation [Acesso em: abril de 2024].

JANUÁRIO, Túlio Xavier – *Inteligência Artificial e Direito Penal da Medicina*. In: RODRIGUES, Anabela Miranda (coord.) – *A Inteligência Artificial no Direito Penal*. Vol. II. Coimbra: Edições Almedina, 2022, pp. 125-173.

KAPLAN, Andreas; HAENLEIN, Michael – *Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence*. *Business Horizons* [online], vol. 62, nr. 1, Jan.–Feb. 2019, pp. 15-25. Disponível em: <https://doi.org/10.1016/j.bushor.2018.08.004> [Acesso em: maio de 2025].

LEITE, André Lamas – Prevenção policial e inteligência artificial no “Direito Penal da (pós-) modernidade”. *Revista LEX de Criminologia & Vitimologia* [online]. Vol. 3, n.º 8 (2023). Disponível em: <https://repositorio-aberto.up.pt/handle/10216/152412> .

LOBATO, Fernanda Silva – *Uso de softwares com função analítica preditiva aplicados à investigação criminal e atividade de inteligência: uma análise sobre o conflito de normas relativas ao direito constitucional à privacidade e à segurança pública* [online]. Trabalho de Conclusão de Curso. Instituto de Ciências Jurídicas, Faculdade de Direito, Universidade Federal do Pará, 2019. Disponível em: <https://bdm.ufpa.br/items/a14265d7-375b-4606-af54-c99e960ceffa/full> [Acesso em: abril de 2024].

LLOYD, John W. – *Foundations of Logic Programming*. 2.^a ed. Berlin: Springer Verlag, 1987.

MARQUES, Garcia; MARTINS, Lourenço – *Direito da Informática*. Coimbra: Almedina, 2000.

MCCARTHY, John; MINSKY, Marvin L.; ROCHESTER, Nathaniel; SHANNON, Claude E. – *A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955*. *AI Magazine* [online], vol. 27, nr. 4, 2006, p. 12-14. Disponível em: <https://doi.org/10.1609/aimag.v27i4.1904> [Acesso em: maio de 2025].

PAIS, Ana – Investigação policial e Inteligência Artificial: o policiamento preditivo e os atuais desafios ao Direito. Em especial, o caso *HessenDATA* e a relevância da decisão do *Bundesverfassungsgericht* de 16 de fevereiro de 2023. In: RODRIGUES, Anabela Miranda (coord.) – *A Inteligência Artificial no Direito Penal*. Vol. III. Coimbra: Edições Almedina, 2022, pp. 167-188.

PEDRINA, Gustavo Mascarenhas Lacerda – *Consequências e perspectivas da aplicação de inteligência artificial a casos penais* [online]. *Revista Brasileira de Direito Processual Penal*, vol. 5, n.º 3, 2019. Disponível em: <https://doi.org/10.22197/rbdpp.v5i3.265> [Acesso em: abril de 2024].

RODRIGUES, Anabela Miranda – A questão da pena e a decisão do juiz – entre a dogmática e o algoritmo. In: RODRIGUES, Anabela Miranda (coord.) – *A Inteligência Artificial no Direito Penal*. Coimbra: Edições Almedina, 2022, pp. 219-244.

RODRIGUES, Anabela Miranda – Em busca da racionalização na determinação da medida da pena – entre a digitalização e a necessidade de um “algoritmo ‘legal’ a ser seguido” (continuação). In: RODRIGUES, Anabela Miranda (coord.) – *A Inteligência Artificial no Direito Penal*. Vol. III. Coimbra: Edições Almedina, 2022, pp. 217-261.

RODRIGUES, Anabela Miranda – Inteligência Artificial no Direito Penal: a Justiça Preditiva entre a Americanização e a Europeização. In: RODRIGUES, Anabela Miranda (coord.) – *A Inteligência Artificial no Direito Penal*. Coimbra: Edições Almedina, 2022, pp. 11-58.

RODRIGUES, Anabela Miranda; FIDALGO, Sónia – Pena de Prisão e Inteligência Artificial – o que esperar de uma aliança (im)provável. In: RODRIGUES, Anabela Miranda (coord.) – *A Inteligência Artificial no Direito Penal*. Vol. III. Coimbra: Edições Almedina, 2022, pp. 263-285.

TURING, Alan. M. – Computing Machinery and Intelligence. *Mind*. Vol. 59, nr. 236 (Oct. 1950), pp. 433-460. Disponível em: <https://doi.org/10.1093/mind/LIX.236.433>.

Ferramentas, notícias e outras fontes

HUTCHINSON, Clare; JOHN, Phil – *AI: Digital Artist's Work Copied More Times Than Picasso*. *BBC News* [em linha]. 20 jul. 2023. Disponível em: <https://www.bbc.com/news/uk-wales-66099850> [Acesso em: junho de 2025].

OED – Oxford English Dictionary [online]. Disponível em <https://www.oed.com/> [Acesso em: maio de 2024].

PASICK, Adam – *Artificial Intelligence Glossary: Neural Networks and Other Terms Explained*. *The New York Times* [online]. 27 mar. 2023. Disponível em: <https://www.nytimes.com/article/ai-artificial-intelligence-glossary.html> [Acesso em: junho de 2025]

PRIBERAM – *Dicionário Priberam da Língua Portuguesa* [online]. Disponível em: <https://dicionario.priberam.org> [Acesso em: maio de 2024].

REILLY, Nick – *Artists Score Major Win in Copyright Case Against AI Art Generators*. *Hollywood Reporter* [online]. 13 ago. 2024. Disponível em: <https://www.hollywoodreporter.com/business/business-news/artists-score-major-win-copyright-case-against-ai-art-generators-1235973601/> [Acesso em: junho de 2025].

ROOSE, Kevin – *An A.I.-Generated Picture Won an Art Prize. Artists Aren't Happy*. *The New York Times* [online]. 2 set. 2022. Disponível em: <https://www.nytimes.com/2022/09/02/technology/ai-artificial-intelligence-artists.html> [Acesso em: junho de 2025].

Legislação nacional e internacional

Carta dos Direitos Fundamentais da União Europeia. Jornal Oficial da União Europeia, C 326, 26 de outubro de 2012, p. 391–407. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12012P%2FTXT>. Acesso em: 3 ago. 2025.

Constituição da República Portuguesa. Disponível em: <https://www.parlamento.pt/Legislacao/Paginas/ConstituicaoRepublicaPortuguesa.aspx>. Acesso em: 3 ago. 2025.

Lei n.º 27/2021, de 17 de maio — Carta Portuguesa de Direitos Humanos na Era Digital (3.^a Versão). Disponível em https://pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=3446&tabela=leis&so_miolo=. Consultada a 27 de junho de 2025.

Livro Branco sobre a Inteligência Artificial — Uma abordagem europeia virada para a excelência e a confiança, COM (2020) 65 final, Bruxelas, 19-02-2020. Disponível em https://commission.europa.eu/document/download/d2ec4039-c5be-423a-81ef-b9e44e79825b_pt?filename=commission-white-paper-artificial-intelligence-feb2020_pt.pdf.

Regulamento (UE) 2024/1689 do Parlamento Europeu e do Conselho de 13 de junho de 2024 – Regulamento Europeu de Inteligência Artificial (AI Act). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202401689. Consultado a 27 de junho de 2025.

Tratado da União Europeia, reformulado pelo Tratado de Lisboa, de 2007, aprovado e ratificado para a ordem jurídica nacional pelo Decreto do Presidente da República n.º 31/2008, de 19 de maio e pela Resolução da Assembleia da República n.º 19/2008, de 19

de maio. Disponível em
<https://dcjri.ministeriopublico.pt/sites/default/files/documentos/instrumentos/rar40-1992.pdf>
f. Consultado a 27 de junho de 2025.