1 2 9 0

INSTITVTO IVRIDICO
FACVLDADE DE DIREITO
VNIVERSIDADE D
COIMBRA

04

Desafios Societais e a Investigação em Direito

Inteligência Artificial

Desafios Societais e a Investigação em Direito

Introdução

A Comissão Europeia, no âmbito da sua política e investimento em Investigação e Desenvolvimento, identificou alguns temas que, dada a sua importância e centralidade, careceriam de ser alvo de projetos: os denominados desafios societais. Essa abordagem visa reunir diferentes disciplinas e tecnologias de diversas áreas para enfrentar questões essenciais no panorama europeu.

Paralelamente, as Nações Unidas apresentaram uma agenda de desenvolvimento para reunir os países e a população global, com o objetivo de trilhar novos caminhos, melhorando globalmente as condições de vida das pessoas. Foram estabelecidos 17 objetivos de desenvolvimento sustentável, com metas a serem alcançadas até 2030.

Para alcançar metas tão ambiciosas e enfrentar desafios complexos é preciso encontrar soluções elaboradas e arrojadas que envolvam diferentes áreas do conhecimento. O Direito pode contribuir de forma transversal para a resposta a vários desafios societais, sendo essencial para a coesão social e a convivência entre as pessoas, bem como para a estruturação de quadros normativos que contribuam para sociedades mais justas.

Este compromisso envolve muitos atores, incluindo as unidades de investigação. O Instituto Jurídico da Universidade de Coimbra visa a excelência no âmbito legal e das ciências sociais, ao produzir investigação dedicada a temas emergentes, resultado de mudanças sociais e políticas contemporâneas. Para enfrentar esses problemas, o Instituto Jurídico definiu três áreas de investigação (Pessoa e o Direito; Direito, Risco e Sociedade Técnica; Transformação do Estado e Globalização) com subdivisões para temas específicos.

Trata-se, por um lado, de assumir um precioso património reflexivo e de prosseguir uma dinâmica exemplarmente instalada na Faculdade de Direito da Universidade de Coimbra. Trata-se, por outro lado, de fortalecer a unidade temática, submetendo a investigação às perspetivas condutoras de um mote tripartido (vulnerabilidade / pluralidade / indecidibilidade), permitindo uma tematização crítico-reflexiva e experimentação prática das possibilidades e limites da resposta ou respostas do Direito a esses desafios.

Inteligência Artificial

O desenvolvimento tecnológico tem provocado aturada discussão a propósito da Inteligência Artificial (IA), acompanhada das possibilidades de concretização de sistemas de IA em robôs e as potencialidades de ordem geométrica criadas pela Internet das Coisas (*Internet of Things*).

Actualmente, a IA integra o nosso quotidiano enquanto cidadãos, tanto em actividades genéricas, bastando pensar no uso do telemóvel e das redes sociais, como em actividades específicas, desde a indústria, às empresas, à administração de Justiça até à prestação de cuidados de saúde.

As preocupações éticas em torno da IA podem sintetizar-se no que se designam as três grandes questões (*Big 3*): *i)* privacidade e vigilância; *ii)* preconceito e discriminação; e *iii)* o papel da decisão humana. Assim, tanto em termos éticos, como em termos legislativos importa saber desenhar uma "IA ético-legal", estabelecendo linhas claras entre o que a IA "pode" (*can*) e o que a IA "deve poder" (*should*) fazer, mantendo sempre uma abordagem em que a IA deve estar ao serviço dos seres humanos, existindo para o seu benefício e não para o seu detrimento.

As preocupações em torno do desenho "ético-legal" da IA têm-se manifestado em termos internacionais, regionais e, mesmo, nacionais.

No patamar internacional, a UNESCO aprovou uma Recomendação sobre a Ética da Inteligência Artificial em 2021, que deve ser respeitada por todos os intervenientes no ciclo da IA. Nesta Recomendação, indicou como grandes valores o respeito, protecção e promoção dos direitos humanos e liberdades fundamentais e da dignidade humana, o florescimento do ambiente e do ecossistema, a garantia da diversidade e da inclusão e a vida em sociedades pacíficas, justas e interligadas. No âmbito do Conselho da Europa, encontra-se em preparação uma Convenção sobre o desenho, desenvolvimento e aplicação de sistemas de IA baseada nos padrões europeus de direitos humanos, democracia e Estado de Direito que, como o nome indica, procurará garantir os eixos fundamentais em que assenta este Conselho.

No patamar regional, têm também existido instrumentos que procuram promover uma IA ética, especialmente a partir de princípios basilares que lhe devem ser aplicáveis: decisão e supervisão humanas, robustez e segurança, privacidade e protecção de dados, transparência, diversidade, não-discriminação e equidade, bem-estar social e ambiental e responsabilidade. Contudo, talvez mais relevante, em termos de União Europeia, seja a proposta de Regulamento sobre Inteligência Artificial, cujo processo legislativo se prevê que fique concluído em breve. A Proposta de Regulamento pretende atingir dois objectivos simultâneos: controlar os riscos associados à IA e aumentar a confiança na IA. Ou seja, o objectivo da Proposta de Regulamento sobre a Inteligência Artificial é permitir um desenvolvimento fiável e seguro da IA na Europa, no pleno respeito pelos valores e direitos dos cidadãos, apresentando dois eixos: por um lado, um ecossistema de confiança, direccionado para a protecção de direitos dos cidadãos e, por outro lado, um

ecossistema de excelência, visando a criação de valor, promovendo o reforço de investimento, inovação e utilização de IA na União Europeia (UE).

Deste modo, a Proposta de Regulamento sobre a Inteligência Artificial pretende estabelecer regras harmonizadas para a colocação no mercado e em serviço de sistemas de IA, proibições de certa IA, regras de transparência harmonizadas para interacção e, ainda, regras de monitorização do mercado e vigilância.

A Proposta de Regulamento sobre a Inteligência Artificial segue uma abordagem baseada na análise de risco ("risk-based approach"). Deste modo, a proposta diferencia entre níveis de risco, designadamente o risco mínimo, o risco limitado, o risco elevado e o risco inaceitável.

O âmbito principal da proposta inscreve-se no patamar do risco elevado. Neste particular, deverão ser considerados de alto risco os sistemas de IA que devam ser usados como componente de segurança de produto ou como produto e que tenham de passar um teste de conformidade para colocação no mercado (p. ex., brinquedos ou equipamento médico). Serão ainda considerados de alto risco os sistemas de IA que se integrem nas áreas de *(i)* identificação biométrica e categorização de pessoas naturais, *(ii)* gestão e operacionalização de infraestruturas críticas, *(iii)* educação e formação profissional, *(iv)* emprego, gestão de recursos humanos e acesso ao emprego, *(v)* acesso e fruição de serviços e benefícios privados ou públicos, *(vi)* aplicação da lei, *(vii)* controlo de fronteiras e migração e *(viii)* administração da justiça e processos democráticos. Estes sistemas de alto risco encontram-se sujeitos a requisitos específicos bastante rigorosos, que procuram criar o necessário equilíbrio entre a utilização de IA e a confiança na IA.

No patamar do risco inaceitável encontramos o âmbito de proibição da proposta, que estabelece os limites da IA permitida, ao identificar os sistemas de IA que constituem um risco inaceitável e, como tal, proibidos, a saber: *(i)* sistemas de IA que usem técnicas subliminares para lá da consciência humana, com vista a distorcer o comportamento de pessoa de forma a causar danos a si ou a terceiros; *(ii)* sistemas de IA que explorem qualquer vulnerabilidade de um grupo específico de pessoas devido à sua idade, deficiência física ou mental, com vista a distorcer o comportamento de pessoas pertencentes a esse grupo, de forma a causar dano, físico ou psicológico, a si ou a terceiros; *(iii)* sistemas de IA, colocados por autoridades públicas, ou a seu pedido, para avaliação ou classificação de confiança de pessoas com base no seu comportamento social; *(iv)* uso de identificação biométrica remota em tempo real em espaços públicos ou de acesso público.

O traço que une todos estes instrumentos, nos diferentes patamares, é a exigência de uma IA antropocêntrica que respeite os valores e princípios civilizacionais assentes da dignidade humana e nos direitos fundamentais.

A IA representa, assim, um grande desafio, não só ao cidadão e à sociedade, como, também, à regulação ético-legal do seu desenvolvimento e utilização por todos, no sentido de ser logrado o necessário equilíbrio entre as suas inegáveis vantagens e os seus riscos.

O I J e a Inteligência Artificial

A Inteligência Artificial é um tema presente em várias discussões científicas e em previsões sobre as áreas que mais irão impactar a sociedade num futuro próximo. Apesar da sua ligação lógica às áreas da tecnologia e informática, o desenvolvimento científico da inteligência artificial precisa estar inserido dentro de um contexto mais amplo, que considere os elementos éticos e humanos do progresso e implementação dessa tecnologia. Se, por um lado, a inteligência artificial oferece grandes oportunidades de futuro, há, por outro lado, situações de risco que precisam ser avaliadas sob um ponto de vista das ciências sociais e humanase, naturalmente, do Direito.

Nesse contexto, o Instituto Jurídico desenvolve investigação sobre a intersecção entre o Direito e a Inteligência Artificial, nas diferentes áreas de aplicação dos conhecimentos das ciências jurídicas. Tal como mencionado no *White Paper* sobre Inteligência Artificial (COM(2020)65), a questão da confiança é um elemento central, de modo que será preciso desenvolver ainda ações que promovam a transparência, capacidade de entendimento e explicação, bem como os níveis de performance esperados. Aqui, o papel do Regulamento Geral da Proteção de Dados poderá ter um papel fundamental.

Como estimulo ao desenvolvimento de investigação na área, o Instituto Jurídico tem vindo a apoiar trabalhos sobre Inteligência Artificial, nomeadamente o projeto exploratório "Inteligência Artificial e Criminalidade Empresarial" (https://www.uc.pt/fduc/ij/projetos-de-investigacao/inteligencia-artificial-e-criminalidade-empresarial/), que resultou na compilação da regulação normativa, num e-book "Artificial Intelligence in the economic sector: prevention and responsability" e num webinário internacional. A atuação do IJ na investigação sobre inteligência artificial é vista como estratégica, de modo que também se procuram ativamente parcerias institucionais internas e internacionais, que já resultaram em candidaturas a financiamento europeu e na organização de eventos em parceria com o Centro de Informática e Sistemas da Universidade de Coimbra (CISUC). Também foram organizadas formações para os investigadores através do Artificial Intelligence Lab Brussels, da Vrije Universiteit Brussel.

Representando apenas parte da investigação sobre Inteligência Artificial realizada no âmbito do Instituto Jurídico, o presente volume recolheu os seguintes textos:

Responsabilidade criminal pelo produto "inteligente": reflexões e desafios | Susana Aires de Sousa; **A utilização de inteligência artificial na obtenção de prova digital em processo penal** | Sónia Fidalgo; **Inteligência Artificial e Cooperação Judiciária Internacional em Matéria Penal: alguns Problemas e Possíveis Respostas** | Miguel João Costa; **Direitos de Autor e Inteligência Artificial** | Alexandre Dias Pereira; **O Direito (Penal), a Ciência e o Paradoxo de Zenão** | Anabela Miranda Rodrigues.

Responsabilidade criminal pelo produto "inteligente": reflexões e desafios

Susana Aires de Sousa— *Investigadora Integrada do Instituto Jurídico*

I. Contextualização: *setting the stage*

Imagine-se um mundo em que os veículos prescindem de condução humana (são, por isso, autónomos), utilizam energia limpa, movendo-se em comunicação com as estradas e outros veículos, interagindo com todo o sistema rodoviário e de transporte. Um mundo onde "as coisas" comunicam entre si, detetando pedestres, prevendo percursos seguros, mais eficientes, e prevenindo (evitando) quaisquer acidentes. Um mundo em que o erro humano é eliminado (estima-se que 94% dos acidentes de trânsito graves têm como causa decisões humanas erradas). Neste cenário, a lesão de bem jurídicos em contexto rodoviário seria reduzida à condição de mero acontecimento fortuito.

Este mundo ainda está por vir, fazendo parte de um futuro provável. O presente, porém, oferece um outro cenário: aquele em que o número de acidentes ligados a carros "inteligentes", autónomos ou automatizados, que circulam sistemas rodoviários desadequados, é crescente, desafiando modelos de responsabilidade e categorias jurídicas clássicas. Um exemplo recente liga-se à manipulação visual de sinais de trânsito, insignificante ao olho humano, mas suficiente para que o algoritmo interprete errada e perigosamente o limite de velocidade permitido. Um outro exemplo, que merece ser referido pela sua visibilidade, mas também por ilustrar os desafios lançados à responsabilidade jurídica, diz respeito ao primeiro atropelamento mortal causado por um carro autónomo da Uber, em fases de testes, ocorrido em março de 2018, em Tempe, no Arizona. A vítima, Elaine Herzberg, foi mortalmente atropelada, quando atravessava uma estrada empurrando uma bicicleta, por um carro, de marca Volvo, modificado pela Uber e autorizado a circular na via pública. Vários fatores contribuíram para este desenlace fatal, desde a dificuldade sentida pelo algoritmo em identificar aquele obstáculo como uma pessoa, reagindo tardiamente, até ao alheamento da *designated driver* – a pessoa humana que no interior do veículo devia monitorizar o seu desempenho –, a uma "cultura empresarial de segurança inadequada", ou ainda à conduta da vítima que atravessava a rodovia, à noite, num local sem sinalização. Em março de 2019, o Ministério Público deduziu acusação por homicídio negligente contra a pessoa humana. O julgamento terá, em breve, lugar.

II. Desafios: o *responsability gap*

As decisões tomadas por algoritmos ocorrem em muitos outros domínios económicos e sociais. A utilização destes sistemas integra o quotidiano por diversas formas, mais ou menos visíveis: meios de informação, comunicação ou aconselhamento (técnico ou económico); *internet*, computadores ou *smartphones*; utilização de sistemas de diagnóstico ou de robôs cirúrgicos; *trading* algorítmico; transportes através de veículos autónomos (carros, *shuttles*, barcos, *drones*), etc. Contudo, decisões tomadas por sistemas computacionais complexos dinâmicos, imprevisíveis à pessoa humana, desafiam modelos e categorias clássicas em que assenta a atribuição de responsabilidade. É justamente nesta autonomia de aprendizagem (e de decisão) que reside o *responsability gap* ou *AI criminal gap*.

Em causa estão as categorias que suportam o juízo de imputação do evento desvalioso a uma conduta, como a causalidade e a culpa. Alguns algoritmos funcionam como autênticas caixas negras na forma como processam os dados (*input*) e alcançam um determinado resultado (*output*). Isto é, o tratamento algorítmico dos dados, segundo uma estrutura complexa, torna opaco o processo que conduz a determinado resultado, não obstante a sua capacidade de grande precisão na determinação de nova informação. A opacidade será tanto maior quanto mais complexos (e precisos) sejam os modelos de *machine learning* utilizados, sendo que, em alguns casos, o estado atual de desenvolvimento tecnológico não permite determinar, atendendo ao grau de complexidade do sistema, como se chegou àquele resultado, seja ele um juízo de previsibilidade, um aconselhamento, ou uma decisão.

Por sua vez, a imprevisibilidade e a natureza dinâmica dos sistemas computacionais complexos fundamentam dúvidas sobre a imputação subjetiva do dano exigida pelos tipos legais de crime. Da perspetiva da pessoa humana ligada ao fabrico, à programação ou à utilização do sistema, a intervenção da máquina

torna imprevisível o evento desvalioso. A opacidade do sistema e a imprevisibilidade do resultado danoso dificultam quer a possibilidade de representação humana daquele resultado, quer uma prova, suficientemente sustentada, da sua existência.

III. Revisitar possíveis soluções

Em alguns casos, as dificuldades podem ser superadas por regras clássicas, já instituídas em contexto de responsabilidade (civil e criminal) pelo produto. Contudo, casos haverá reveladores de especiais particularidades associadas à complexidade computacional do produto dito "inteligente". Este produto distingue-se, no risco que lhe é inerente, pela sua imprevisibilidade e incontrolabilidade. O *risco inerente* é um conceito importante em matéria de responsabilidade pelo produto porque constitui um parâmetro para a intervenção do direito enquanto instrumento de controlo de riscos. A grande autonomia de alguns sistemas inteligentes, associada ao contexto em que são aplicados (por exemplo, tráfego rodoviário) ou às circunstâncias em que são utilizados (*v. g.*, domínio militar), impõe um dever acrescido de cuidado que deve concretizar-se em medidas jurídicas que diminuam esse risco, procurando-se, dessa forma, aumentar a *confiança* numa utilização segura, capaz de modificar o grau de risco para um nível aceitável ou permitido.

Deste modo, em casos de incerteza sobre a amplitude dos riscos associados ao produto "inteligente", o princípio da precaução constitui fundamento para a imposição de medidas e deveres especiais, como um dever de vigilância e monitorização do produto ou a implementação de regulação dinâmica (*v. g.*, a *sandbox aproach)*. Estas medidas contribuem para um conhecimento gradual do produto em contexto real, diminuindo assim a sua opacidade (ou *black box*).

Estes deveres, assentes numa ideia de plausibilidade do risco, são imputáveis a pessoas jurídicas (humanas e empresas), cujo cumprimento pode ser reforçado por normas sancionatórias, essencialmente de natureza não penal. Todavia, esta regulação deve estar sujeita a um *princípio de revisibilidade* que acompanha o grau de conhecimento do produto. Ou seja, na medida em que o contexto de plausibilidade evolua para um estado de previsibilidade, deve rever-se a necessidade de intervenção penal. Assim, se o risco de produção do dano se torna previsível, deve a autoridade pública averiguar da necessidade de criminalização da conduta, designadamente através da construção de incriminações especificamente voltadas para a chamada *IA forte*.

A utilização de inteligência artificial na obtenção de prova digital em processo penal

Sónia Fidalgo — *Investigadora Integrada do Instituto Jurídico*

1. No passado, os tribunais mostraram-se hesitantes em aceitar que a prova dos factos em processo penal fosse feita através de meios tecnológicos. Porém, o uso continuado e generalizado de tecnologia cada vez mais sofisticada parece ter provocado uma mudança de atitude no sistema de administração da justiça penal.

Atualmente, grande parte da vida de cada um de nós deixa um *rasto digital* que se encontra armazenado em sistemas informáticos de diversa natureza. Além disso, há uma ampla quantidade de informação que circula nas redes informáticas, redes estas que são também locais privilegiados para a prática de crimes. Compreende-se, deste modo, o interesse em aceder a estes sistemas informáticos para recolher prova da prática de crimes e determinar quem foram os seus agentes. Não surpreende, assim, que a prova digital tenha entrado nos tribunais e que esteja hoje presente na generalidade dos processos de natureza criminal.

2. A prova digital é, por natureza, uma prova imaterial, frágil e volátil. Neste contexto, tem vindo a desenvolver-se um método científico de identificação, recolha e análise de provas em ambiente digital - a *ciência forense digital* -, de modo a que estas possam vir a ser validamente apresentadas em tribunal.

No momento presente, o aumento da capacidade dos meios de armazenamento digital e a disseminação destes meios na vida diária de todos nós têm-se traduzido, por um lado, num aumento do número de pedidos de análise e recolha de dados que é feito no âmbito do processo penal e, por outro lado, têm representado um aumento do volume de dados a analisar.

E as ferramentas *tradicionais* da ciência forense digital não são suficientemente robustas para analisar uma tão grande quantidade de dados, nem para estabelecer as necessárias correlações entre eles. Consequentemente, o trabalho dos especialistas tem vindo a tornar-se cada vez mais difícil e moroso, destacando-se uma clara assimetria entre as técnicas cada vez mais sofisticadas utilizadas para a prática de crimes, sobretudo no ciberespaço, e as ferramentas utilizadas na ciência forense digital.

3. A inteligência artificial apresenta-se, assim, como a *solução ideal* para resolver alguns dos problemas com que se confronta hoje a ciência forense digital. Os sistemas de inteligência artificial, através da análise e correlação de dados, permitem reduzir a quantidade de dados a analisar pelos especialistas; permitem encontrar ligações entre dados, que, tendo em conta a enorme quantidade de dados a analisar, podem passar despercebidos aos especialistas; e reduzem (em geral) a possibilidade de ocorrência de erros em todo o processo de aquisição, preservação, análise e interpretação dos dados.

4. A utilização destas novas realizações tecnológicas em processo penal tem, porém, um preço. Alargando o arsenal de meios de investigação do crime e de perseguição do criminoso, a utilização de inteligência artificial no domínio da prova digital traduz-se num claro atentado a uma multiplicidade de direitos dos atingidos.

4.1. O direito à privacidade está, naturalmente, entre aquelas cuja violação é mais evidente. É certo que o direito processual penal prevê, em geral, a possibilidade de limitação do direito à privacidade em nome dos interesses da investigação. Mas o âmbito daquilo que é previsto pelas normas que regulam os meios de obtenção da prova fica, atualmente, muito aquém daquilo que as novas tecnologias permitem.

No tempo presente, uma parte substancial de dados da nossa privacidade encontra-se em dispositivos eletrónicos que seguem, em tempo real, os nossos movimentos. Vivemos hoje como que uma *duplicação da nossa identidade*: à *identidade física* acresce aquilo a que já se chama a *identidade digital*. As normas que regulam a possibilidade de intromissão na privacidade com finalidades de investigação criminal tornaram-se, em grande parte, desadequadas.

Perante esta nova realidade, é importante não esquecer que a compressão de direitos fundamentais em nome da descoberta da verdade material estará sempre dependente da intervenção do legislador, sob pena de a prova indevidamente obtida dever ser considerada prova proibida.

4.2. Mas, ainda que da perspetiva da proteção da privacidade se admita – mediante a devida intervenção legislativa - a utilização de técnicas de inteligência artificial na obtenção de prova digital em processo penal, um outro problema fica ainda por resolver. Atendendo à complexidade que carateriza as técnicas de inteligência artificial, cabe questionar se estará salvaguardado o direito de defesa do arguido quando tais técnicas são utilizadas na obtenção da prova.

Para que o direito de defesa se considere assegurado, a oportunidade que é dada ao arguido para contrariar a prova tem de ser efetiva e eficaz. Quando para obter a prova tiverem sido utilizadas técnicas de inteligência artificial, a possibilidade de contrariar esta *prova automatizada* estará claramente prejudicada. Para que possam ser usados sistemas de inteligência artificial na obtenção da prova em ambiente digital, os sistemas de utilizados terão de ser sempre *explicáveis* e *transparentes*: apenas a utilização de sistemas de inteligência artificial com estas características permitirá alcançar o equilíbrio entre os interesses da investigação e a proteção do direito de defesa do arguido.

5. A descoberta da verdade constitui uma das finalidades do processo penal. Em processo penal, porém, os factos não podem ser provados do mesmo modo por que se provam os factos no domínio científico. Para que o processo penal seja *justo* e *leal* tem de haver um confronto oral em audiência de julgamento, em que as provas apresentadas possam ser contrariadas pelos diversos sujeitos processuais (*maxime*, pelo arguido).

Não podemos recusar a intervenção das realizações tecnológicas no processo penal, mas também não podemos perder de vista o direito à privacidade, o direito de defesa e a presunção de inocência de que goza o arguido. Só através de um diálogo sério entre juristas e cientistas poderemos almejar encontrar um (*renovado*) equilíbrio entre a descoberta da verdade material e a realização da justiça, por um lado, e a proteção dos direitos fundamentais do arguido, por outro.

Inteligência Artificial e Cooperação Judiciária Internacional em Matéria Penal: Alguns Problemas e Possíveis Respostas

Miguel João Costa — *Investigador Integrado do Instituto Jurídico*

1. Os impressionantes desenvolvimentos recentemente registados no domínio da IA têm recebido séria reflexão por parte de várias organizações de referência, como a UE, a ONU e o Conselho da Europa, cujo Comité para os Problemas Criminais, por outro lado, também identifica actualmente como prioritária a cooperação judiciária internacional em matéria penal. Embora antiga, esta última área é particularmente sensível aos desenvolvimentos tecnológicos, não surpreendendo, por isso, que figure juntamente com a IA e o cibercrime numa lista de prioridades da justiça penal na entrada da terceira década do século XXI. Esse tipo de desenvolvimentos perturba a clássica correspondência entre soberania e território, dificultando o exercício de soberania por parte dos Estados mesmo em relação à sua própria criminalidade doméstica. A intervenção de outros Estados nesse tradicionalmente autónomo exercício passou a ser normal.

Através da extradição e da transmissão de processos, da execução de sentenças estrangeiras e do auxílio judiciário mútuo, a cooperação internacional pode ser chamada a intervir na prevenção e na investigação de crimes, no seu julgamento e na execução das sanções aplicadas. Emergem daí problemas como o da validade da prova obtida no estrangeiro ou o de saber que consequências deve ter a inobservância de direitos fundamentais nos processos aí realizados. O próprio conceito de crime é convocado ao debate, através da regra da dupla incriminação.

2. Uma das mais clássicas regras desta matéria, a dupla incriminação determina que um Estado apenas coopere com outros Estados por factos que ele próprio criminaliza. É uma das regras que logo se vê aqui interpelada, porque do desenvolvimento da IA emergem novos crimes. Não apenas relativos a condutas novas (*v.g.* ataques danosos à normal operação de sistemas de IA ou à sua interacção com seres humanos, ou condutas relacionadas com a produção e utilização de veículos autónomos); também a condutas já conhecidas e geralmente não criminalizadas, mas cuja danosidade social pode ser radicalmente ampliada pela intercessão da IA e passar a reclamar criminalização (*v.g.* a difusão de *fake news* e outras formas de manipulação de informação, como a automação e a hiper-personalização de campanhas de influência).

Apesar da expectável definição de parâmetros regionais e internacionais comuns, é inevitável a subsistência de alguma disparidade regulatória – visto que a criminalização de condutas é em última instância efectuada no plano nacional, com as adaptações impostas pela tradição jurídica local – e, onde houver disparidade, a dupla incriminação tenderá a inviabilizar a cooperação. Isso acontece já com a criminalidade 'tradicional', mas pode defender-se que assume agora contornos algo distintos. No âmbito tradicional, a criminalização reflectirá de um modo mais afinado aquilo que uma dada comunidade considera merecedor de punição, surgindo a ausência de criminalização como um espaço de liberdade intencionalmente proporcionado. Já em outros domínios, esse espaço pode simplesmente constituir uma inadvertida lacuna de punição relativamente a condutas de cuja danosidade um Estado ainda não se deu conta mas cuja criminalização não ofenderia os seus princípios fundamentais. Em domínios novos, dinâmicos e de forte potencial de impacto social (vectores estes à luz dos quais a IA se vê colocada no mesmo plano de outros temas prioritários, como o da tutela do ambiente pela via penal), pode, dentro de certos limites, justificar-se a assistência a outros Estados mesmo por factos que não se criminaliza.

Claro que, para a questão de saber quando pode punir-se criminalmente uma pessoa, aquela diferença entre espaços de liberdade intencionais e inadvertidos é irrelevante: só pode punir-se o que constituía crime. No plano da cooperação, porém, não está ainda em causa uma punição, mas a questão de saber até que ponto pode auxiliar-se outro Estado a aplicá-la relativamente a condutas que aí foram cometidas e que aí eram criminalizadas. A generalidade dos Estados continua a reconhecer que a territorialidade é a conexão preponderante e a regra dupla incriminação não pressupõe um consenso perfeito entre dois Estados quanto à definição dos crimes.

3. Outro amplo conjunto de questões prende-se com a utilização da IA em juízos de prognose. Em vários planos: no pré-processual (*v.g.* com o *predictive policing*); no processual (*v.g.* nas medidas de coacção, para calcular o risco de fuga); no da determinação

da sanção (*v.g.* nas medidas de segurança, para determinar a perigosidade criminal); no da execução da sanção (*v.g.* no âmbito da liberdade condicional, para auxiliar nos juízos de prevenção geral e especial).

Como noutras vertentes da utilização da IA, o problema está em conciliar a grande eficiência na administração da justiça que essa utilização promete e os grandes riscos para os direitos fundamentais que lhe vêm associados (*v.g.* para a privacidade, os direitos de defesa, a presunção de inocência e a independência judicial). Alguns destes riscos poderão ser mitigados satisfatoriamente, mas a incerteza e a indefinição são as notas dominantes num momento em que se dão ainda os primeiros passos legislativos e jurisprudenciais.

A questão fundamental que todos estes desenvolvimentos colocam ao tema aqui em causa é a de saber se deve prestar-se assistência a outros Estados relativamente a processos penais onde tenham sido ou possam vir a ser utilizados mecanismos com os propósitos indicados. Para Estados, como o português, que deles praticamente não fazem ainda uso interno, a necessidade de tomar posição poderá surgir através de um pedido de cooperação internacional. Como decidir, por exemplo, um pedido de extradição de uma pessoa para cumprimento de uma pena aplicada no âmbito de um processo penal onde a generalidade da prova foi recolhida por sistemas de IA operando segundo critérios opacos?

Os instrumentos jurídicos em matéria de cooperação obrigam os tribunais a recusar a cooperação quando o Estado estrangeiro não assegure determinados padrões de protecção de direitos fundamentais, mas não é ainda claro em que medida aqueles mecanismos violam esses instrumentos. Neste contexto de incerteza, a intervenção dos órgãos político-administrativos no processo de cooperação poderá evitar a colaboração do Estado em condenações de duvidosa justiça, o que não poderia ser evitado pelos órgãos judiciais, adstritos como estão a aplicar normas que por definição se desenvolvem a um ritmo mais lento do que os desenvolvimentos em causa.

Direitos de Autor e Inteligência Artificial

*Alexandre Dias Pereira** — *Investigador Integrado do Instituto Jurídico*

A Inteligência Artificial (IA) coloca vários desafios ao Direito de Autor.[1] A Organização Mundial da Propriedade Intelectual (OMPI/WIPO) lançou uma consulta pública sobre questões que a inteligência artificial coloca à propriedade intelectual e que poderá conduzir à adoção de um instrumento de direito internacional[2].

Para começar, a IA não apenas auxilia a criação intelectual humana, mas também é já capaz de gerar autonomamente obras literárias ou artísticas. Tenham-se em mente, por exemplo, os projetos *The Next Rembrandt*, na pintura, ou o *Deep Mind*, da *Google,* na composição musical. Serão estas obras protegidas pelos direitos de autor?

Depois, na realização dessas obras, a IA utiliza obras e outros conteúdos protegidos por direitos de autor e/ou direitos conexos. A utilização dessas obras pela IA é livre ou, pelo contrário, está sujeita igualmente a direitos de autor relativamente aos conteúdos que utiliza?

Finalmente, a IA é uma ferramenta poderosa ao nível do controlo da licitude de utilização de conteúdos protegidos por direitos de autor e conexos, em especial nas plataformas de partilha online. Qual será o papel destas tecnologias a este nível? Será a comunicação online regida por robôs de direitos de autor?

Na União Europeia, o Parlamento Europeu (PE) adotou no dia 20 de outubro de 2020 uma resolução sobre «os direitos de propriedade intelectual para o desenvolvimento de tecnologias de inteligência artificial»[3], na qual defende uma "abordagem antropocêntrica à IA que respeite os princípios éticos e os direitos humanos" (para. E). Não obstante toda a harmonização legislativa na União Europeia, o Parlamento Europeu defendeu a necessidade de um novo instrumento especialmente dedicado às questões da IA, na forma de um *regulamento* e seguindo uma *abordagem antropocêntrica* na substância.

Nesta ordem de ideias, parece-nos que a obra literária ou artística, enquanto fruto da liberdade de criação cultural, está umbilicalmente ligada ao espírito humano, pelo que as obras geradas por IA não serão protegidas por direitos de autor, embora possam ser objeto de direitos conexos, como os direitos do produtor de fonogramas e de videogramas e, bem assim, do fabricante de bases de dados. Alguns casos, como as obras de artes plásticas ou os programas de computador desenvolvidos autonomamente por sistemas de IA, poderão revelar lacunas de proteção, face à tipicidade fechada dos direitos exclusivos. Todavia, assim como a natureza gera obras de arte com valor estético incalculável, sem que os direitos de autor protejam essas obras nem haja necessidade de as proteger, também não custa aceitar que a IA gere obras à nascença livres de direitos. Assim, o Regulamento deveria centrar-se na obra literária ou artística como fruto da liberdade de criação intelectual da pessoa humana, sem prejuízo da atribuição de direitos conexos, nomeadamente aos produtores de conteúdos audiovisuais, como forma de proteger e estimular os investimentos em sistemas de IA.

Por outro lado, a promoção da aprendizagem e da criatividade da IA não beneficia de um livre trânsito de direitos de autor, no sentido de que a utilização pela IA de obras protegidas deve conformar-se com as leis de direitos de autor e conexos, nomeadamente. Não obstante, nos termos da Diretiva 2019/790[4], os *cérebros de silício* beneficiam de um regime de direitos de autor que permite a utilização de obras através de prospeção de textos ou dados (*machine learning*). Os sistemas de IA poderão analisar automaticamente textos e dados em formato digital, a fim de, com base nessa análise, produzir informações, tais como padrões, tendências e correlações, entre outros.

* Universidade de Coimbra, Professor da Faculdade de Direito e Investigador do Instituto Jurídico.

1 *Vd.* Alexandre Dias PEREIRA, «Os direitos de autor e os desafios da inteligência artificial: copyright *ex machina*?», *Revista de Legislação e de Jurisprudência*, 150/4025 (2020), p. 66-84, e «Editorial: A copyright 'human-centred approach' to AI?», *GRUR - International*, 70/4 (2021), p. 323-324.

2 «Impact of Artificial Intelligence on IP Policy: Call for Comments», <https://www.wipo.int/about-ip/en/artificial_intelligence/call_for_comments/index.html#issues>

3 <https://www.europarl.europa.eu/doceo/document/TA-9-2020-0277_PT.html>

4 Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho de 17 de abril de 2019 relativa aos direitos de autor e direitos conexos no mercado único digital e que altera as Diretivas 96/9/CE e 2001/29/CE.

Finalmente, os sistemas de identificação e bloqueio de conteúdos (*filtros de copyright*) afirmam-se como a tecnologia padrão para controlar a violação nas plataformas de partilha de conteúdos e redes sociais, sendo humanamente impossível substituir os robôs da internet. Ao invés do olho humano, o controlo é feito através de software de identificação e bloqueio/remoção de conteúdos, pelo que é cada vez mais importante a chamada ética algorítmica. Tanto mais que as leis de direitos de autor estabelecem utilizações livres de obras protegidas, para fins, nomeadamente, de ensino e aprendizagem, informação, investigação científica, crítica, paródia, arquivo e documentação, ou bibliotecas. Estas utilizações livres densificam outros valores com dignidade constitucional, como sejam a liberdade de ensinar e de aprender, a liberdade de informação e de expressão, a liberdade de investigação científica e, em última análise, a própria liberdade de criação cultural[5], já que, tal como na Natureza, também na Cultura "nada se cria, tudo se transforma". Daí a importância de garantir o controlo humano da IA e de assegurar o recurso a vias judiciais para a efetivação dos direitos e liberdades dos utilizadores, como sejam a liberdade de expressão e o direito à privacidade e à proteção dos dados pessoais, ao invés de confiar cegamente o sistema a uma espécie de *IUS EX MACHINA*.[6]

5 *Vd.* Alexandre Dias Pereira, *Direitos de Autor e Liberdade de Informação*, Almedina, Coimbra, 2008.

6 *Vd.* Alexandre Dias Pereira, «As plataformas comerciais de partilha em linha de conteúdos digitais e os direitos de autor na União Europeia», Revista de Direito Intelectual 1-2022, p. 59-94, e «Upload filters for 'obvious' infringement», Comunicação apresentada no *Congresso ALAI Direito de Autor, Direitos Conexos e Especiais*, Estoril, 15 e 16 de setembro de 2022 (em publicação)

O Direito (Penal), a Ciência e o Paradoxo de Zenão

Anabela Miranda Rodrigues — *Investigadora Integrada do Instituto Jurídico*

Não nos devemos deixar iludir pelo paradoxo de Zenão, em que por mais que Aquiles (a *Ciência*) corra, sempre haverá um espaço a separá-lo da tartaruga (o *Direito*) e não conseguirá vencer a corrida. Contra as evidências dóxicas em que a sociedade algorítmica nos quer fazer crer, o Direito tem de ser pensado. Ele é desafiado nos seus princípios e conceitos, normatividade e metodologias - as definições surgem vagas e indeterminadas, as soluções legais não abarcam os problemas e os processos de decisão escapam ao domínio humano. No contexto de novas respostas do Direito para os problemas colocados pela IA o debate é intenso.

A viragem digital trouxe consigo duas premissas para aumentar exponencialmente a utilização de algoritmos em toda a espécie de tomadas de decisões, também no mundo da justiça – produção maciça de dados e poder computacional de cálculo, num quadro de globalização de redes. Isto permitiu oferecer ao Direito instrumentos que lhe são de enorme utilidade e que não param de evoluir. A IA está na corrida e alimenta-se ainda do melhor conhecimento sobre o nosso cérebro, que as neurociências ou a economia comportamental favorecem. Os riscos desta abertura às novas fronteiras do desenvolvimento tecnológico e de aplicação de sistemas de IA às nossas vidas são inevitáveis e necessita-se de um fio condutor que nos oriente na busca de um Futuro Humano.

O direito penal está particularmente exposto a estes desenvolvimentos - nas suas categorias dogmáticas, nas incriminações que conhece, no domínio processual, na administração da justiça e da perspetiva internacional e transnacional.

Identificam-se temas continuadamente merecedores de atenção. É o caso da atribuição da responsabilidade penal a pessoas individuais ou coletivas ou a agentes artificiais, designadamente, perante a digitalização empresarial ou em face da utilização de veículos autónomos. Como se vem fazendo notar, a questão é menos teórica do que se possa pensar. Apesar de se falar em golpe publicitário, um *software* de IA – *Vital* – foi, em 2014, nomeado com o estatuto de observador, com direito a voto, para o Conselho de Administração da empresa de capital de risco, sediada em *Hong-Kong*, *Deep Market Ventures*. Apesar de já ter sido «despedido», na Europa, pelo menos numa empresa, a finlandesa *Tieto*, é assinalado o caso de um artefacto de IA autónomo semelhante – *Alicia T* – como membro de uma equipa de direção com direito a voto. E foi a falta de uma teoria da responsabilidade que levou à não acusação no caso *Uber*, quando um dos seus veículos autónomos atropelou e matou um pedestre no *Arizona*.

No setor económico-financeiro, onde é crescente a incorporação da IA na prossecução mais eficiente dos seus fins, não só ao nível do processo produtivo, mas também do *compliance* – fala-se de compliance inteligente e preditivo -, sobressai, simultaneamente, a sua ambivalência. Tornam-se mais visíveis cenários de riscos associados à utilização de IA, tais como o risco sistémico, de discriminação, de fraude, de violação da privacidade, de híper-vigilância e de manipulação e, no plano estritamente processual penal, discute-se a validade do princípio da presunção de inocência e o aproveitamento para fins penais de informação recolhida por formas de monitorização inteligente à custa da limitação de direitos fundamentais das pessoas envolvidas. E os desafios são do mesmo teor se pensarmos na área da medicina, onde a IA é já uma presença omnipresente e omnipotente. Desde a medicina personalizada e preditiva, passando por meios de auxílio de diagnóstico e de predição de suicídio, até ao desenvolvimento de robôs de auxílio ao tratamento e em cirurgias, num contexto de interação entre agentes humanos e artificiais inteligentes, o problema da atribuição de responsabilidade penal ressurge e reequacionam-se aspetos relativas à tutela da privacidade dos pacientes no que toca aos seus dados pessoais e à informação e consentimento à luz da garantia à transparência dos procedimentos que envolvem IA.

Neste feixe de temas de preocupação para o direito penal, não se esquecem os *crimes de fantasia* (*fantasy crimes*) – condutas no mundo virtual que constituiriam crime se fossem praticadas no mundo real. E se um avatar viola outro avatar? Somos confrontados com o cibercrime e os crimes no metaverso, onde estas e outras interrogações sobressaem e se procuram distinguir, à luz da função do direito penal,

as condutas do mundo virtual que produzem ofensas no mundo real das que produzem ofensas apenas no mundo virtual. Além disso, incriminações clássicas, como o abuso de mercado, são postas à prova como resultado do envolvimento da IA na sua prática – designadamente, através da negociação algorítmica de alta frequência (HFT), no caso do abuso de informação, interpelando conceitos tidos por estabilizados de informação privilegiada ou de investidor razoável; ou, no caso da manipulação de mercado, convocando a alteração do tipo legal, mediante o recurso à utilização de um elemento subjetivo da ilicitude «intenção de manipulação do mercado». Já no âmbito do direito da guerra, o desenvolvimento e a utilização das Armas Autónomas Mortíferas (AAMs), vistas como a 3ª grande revolução na história militar, depois da pólvora e das armas nucleares, colocam problemas particulares que os princípios e o direito da guerra tradicionais não resolvem.

Deve sublinhar-se, ainda, que a IA trouxe uma *nova* previsibilidade à justiça penal. Fala-se de *justiça preditiva*, que atravessa todo o sistema, desde a atividade policial, passando pela investigação e a produção de prova e atingindo o processo de tomada de decisões, quer pelo que toca às partes, onde a *Legaltech* tem conhecido um grande desenvolvimento na advocacia, quer quanto aos decisores judiciários, onde é crescente a utilização de instrumentos de avaliação de risco. De momento, mais utilizados em ordenamentos de *common law*, no âmbito da *parole*, em decisões de *bail* ou de *sentencing* (o caso *Loomis* é já um *leading case*), os sistemas continentais também já os conhecem. Discute-se, em última análise, a possibilidade de um juiz robô – é conhecido o projeto *Velsberg*, aprovado na Estónia. A questão prende-se com o facto de os juízes decidirem sobre a culpa e a punição a aplicar. E passa pelo *determinismo* que o digital imprime ao direito. Esta transformação, pelo lado do juiz, retira à decisão a dimensão humana e de responsabilidade que, como tal, envolve encontrar o sentido jurídico – a interpretação; pelo lado do delinquente, a lei torna-se individual e muda - esta passa a ser uma injunção individual e a capacidade de transformação daquele é supérflua – e a punição desliga-se do facto praticado e passa a ser baseada no risco que o indivíduo representa para a sociedade.

Por fim, é preciso ter presente que, pelo que diz respeito às matérias de jurisdição territorial e de cooperação judiciária, os desenvolvimentos da IA da perspetiva transnacional trazem novas dimensões aos problemas de conflitos positivos de jurisdição territorial e de lacunas de cooperação e do respeito pelos direitos fundamentais.

Dezembro de 2022

Este trabalho é financiado por Fundos Nacionais através da FCT – Fundação para a Ciência e a Tecnologia no âmbito do «Projeto do Instituto Jurídico UIDB/04643/2020»

FCT
Fundação para a Ciência e a Tecnologia
MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E ENSINO SUPERIOR