



ANDERSEN®

Newsletter

PI, PRIVACIDADE E NEGÓCIOS DIGITAIS

Outubro 2026

Atualidade e perspectivas

Uma seleção de conteúdos e análises sobre os principais desenvolvimentos em Propriedade Intelectual, Privacidade e Negócios Digitais.

Index

Andersen in Portugal

- 04 IA E DECISÕES AUTOMATIZADAS**
O ser humano como última fronteira
João de Sousa Guimarães | Partner
- 07 DADOS PESSOAIS E INTERESSE LEGÍTIMO**
Fundamentos de licitude para o treino de sistemas de IA
Augusto Almeida Correia | Director
- 10 IMPACTO DA NIS2 NO SETOR DA SAÚDE**
Em particular nos Dispositivos Médicos e Ensaios Clínicos
Daniel Torres Gonçalves | Partner
- 13 IA E A PROSPECÇÃO DE TEXTOS E DADOS**
As novas exceções ao direito de autor na Europa
Gonçalo Gil Barreiros | Local Partner



Subscriba

Se quiser receber as atualizações sobre Propriedade Intelectual, Privacidade e Negócios Digitais elaboradas pela equipa da Andersen, pode inscrever a nossa newsletter através **deste formulário**.



A Inteligência Artificial deixou de ser um debate sobre um assunto do futuro para se tornar uma realidade dos nossos dias, desde os sistemas que aprovam um crédito, nos algoritmos que selecionam candidatos num processo de recrutamento, nas ferramentas que já auxiliam diagnósticos médicos e em diversas plataformas relacionadas com o apoio à tomada de decisões judiciais.

A velocidade com que estes sistemas passaram a proliferar superou, em muito, a capacidade de as organizações — e do próprio Direito — acompanharem o que está, afinal, a ser delegado aos sistemas de informação. E é precisamente dessa delegação que nasceu a necessidade de abordar vários aspetos que este artigo coletivo se propõe explorar.

A questão não é, pois, tecnológica. É, antes de tudo, humana.

Quando um sistema de inteligência artificial produz um resultado — uma recomendação, uma pontuação, uma decisão — o que acontece a seguir? Será que existe uma pessoa que a lê, a compreende, a questiona ou assume? Ou existe apenas alguém que a valida, por inércia ou por confiança cega num algoritmo, aquilo que uma máquina ou um sistema já concluiu?

O legislador europeu tomou posição clara: o RGPD e o AI Act constroem, em conjunto, um edifício jurídico que coloca a supervisão humana efetiva no centro dos sistemas de alto risco, não como uma formalidade, outrossim como exigência. Porque uma intervenção humana sem compreensão não é supervisão — é cumplicidade passiva.

Há, todavia, uma dimensão que o debate regulamentar ainda não esgotou — e que os autores deste artigo não resistiram a deixar em aberto. Se delegarmos sistematicamente nas máquinas as decisões mais complexas, o que acontece à nossa própria capacidade de as tomar? A atrofia cognitiva dos operadores que deixam de exercitar o julgamento crítico não é uma hipótese distópica: é um risco real e reconhecido. Garantir que o ser humano permanece no centro da decisão não é, por isso, apenas uma obrigação jurídica — é uma questão de sobrevivência intelectual. E o Direito tem um papel essencial na sua preservação.



IA e decisões automatizadas

O ser humano como última fronteira

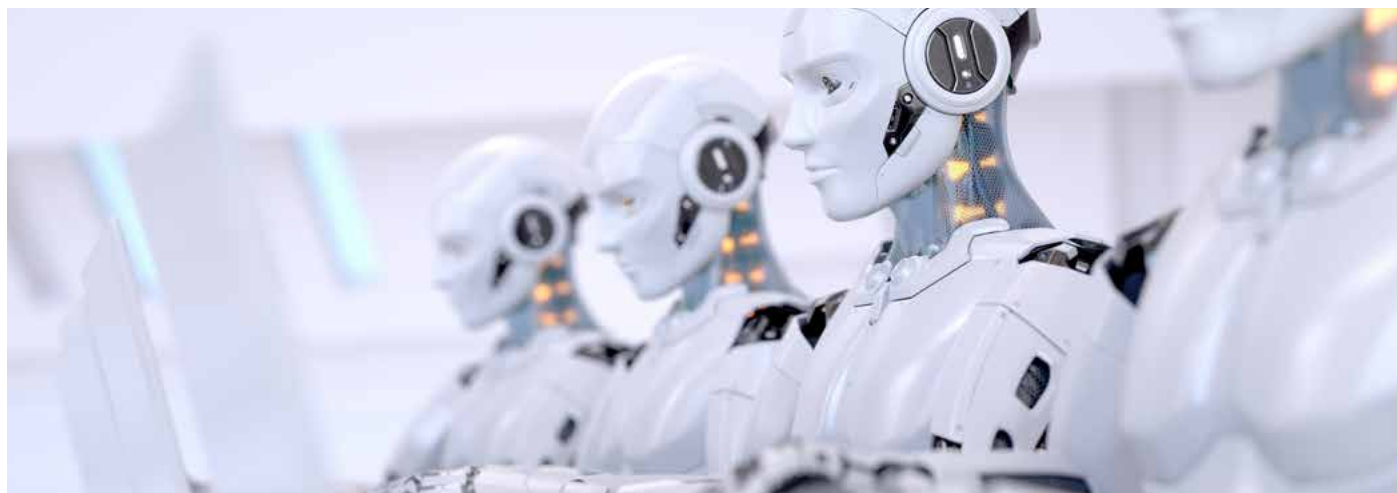


João de Sousa Guimarães

Partner | Corporate and M&A

✉ joao.guimaraes@pt.Andersen.com

Vivemos num mundo que decide sobre nós mais depressa do que conseguimos reagir. Um algoritmo avalia se merecemos um crédito. Outro decide se o nosso perfil encaixa numa vaga de emprego. Outro ainda determina se somos candidatos a um tratamento médico ou a uma análise fiscal. A tomada de decisões automatizada e a definição de perfis tornaram-se uma infraestrutura silenciosa do quotidiano. Desde a banca à saúde, da fiscalidade aos seguros, à administração pública, todos recorrem cada vez mais à tecnologia para “ajudar” a decidir. Mas a questão não é se a inteligência artificial decide — porque já o faz. A questão é saber se existe alguém, no final do processo, que assuma verdadeiramente essa decisão como sua.



I. O que decide por nós hoje

O RGPD estabelece o conceito de definição de perfis como a forma de tratamento automatizado de dados pessoais destinado a avaliar os aspetos pessoais de um titular de dados, designadamente para analisar ou prever o seu desempenho profissional, situação económica, saúde, preferências, comportamento, localização ou deslocações. Na prática, o processo tende a seguir três fases: recolha de dados, análise automatizada para identificar correlações e aplicação dessas correlações a um indivíduo concreto para inferir características presentes ou futuras.

O que é, pois, decisivo não é a sofisticação do sistema a que se recorre, mas o seu impacto e no quanto pode afetar significativamente alguém. E uma decisão afeta significativamente um titular de dados pessoais quando é suscetível de alterar as suas circunstâncias, o seu comportamento, as suas escolhas, de produzir efeitos prolongados ou permanentes, ou ainda de conduzir à sua exclusão ou discriminação. O considerando 71 do RGPD cita como casos paradigmáticos a recusa automática de crédito ou processo de recrutamento sem intervenção humana. Por detrás desses exemplos há vidas reais, percursos interrompidos, oportunidades negadas por um sistema que não pergunta.

II. O artigo 22.º do RGPD: uma linha vermelha

O artigo 22.º, n.º 1, do RGPD reconhece o direito a não ser objeto de uma decisão baseada exclusivamente no tratamento automatizado — incluindo a definição de perfis — quando produza efeitos jurídicos ou afete de modo igualmente significativo. As Diretrizes do Comité Europeu para a Proteção de Dados esclarecem que não se trata de um direito que o titular tenha necessidade de invocar: opera, antes, como uma proibição geral aplicável sempre que se verifiquem os seus requisitos.

Uma decisão é “baseada exclusivamente” em tratamento automatizado quando não tenha havido intervenção humana real no processo. Se alguém analisa e pondera outros fatores antes de decidir, já não é aplicável essa qualificação.

Mas o RGPD não se contenta com um ser humano decorativo. Para que a intervenção seja válida, deve ser significativa, levada a cabo por alguém com a capacidade necessária para alterar o resultado depois de avaliar todos os dados relevantes disponíveis. Validar automaticamente aquilo que um algoritmo já calculou não é supervisão.

A proibição só cede em três situações devidamente tipificadas: quando a decisão seja necessária para a execução de um contrato, quando seja autorizada pelo Direito da UE ou de Estado-Membro com salvaguardas adequadas, ou quando se baseie no consentimento explícito do titular.

Mesmo nesses casos, o artigo 22.º, n.º 3, exige um mínimo irrenunciável: o direito a obter intervenção humana, a expressar o seu ponto de vista e contestar a decisão. E essa revisão deve poder alterar o resultado.



III. O AI Act: supervisão humana como obrigação estrutural

Por seu turno, o Regulamento da Inteligência Artificial (AI Act) transforma a supervisão humana num requisito de conceção para os sistemas de alto risco, no sentido de deverem ser construídos de modo a poderem ser efetivamente supervisionados por pessoas durante a sua utilização. Quem supervisiona deve compreender as capacidades e os limites do sistema, deve monitorizar o seu funcionamento e detetar as suas anomalias. Mas não apenas: deve ainda estar alerta para o chamado “viés de automatização” — a tendência humana para confiar em excesso no resultado produzido —, ser capaz de interpretar corretamente os resultados obtidos, a capacidade real de ignorar, substituir ou reverter a saída do sistema, e até de o deter.

O AI Act classifica, assim, como de alto risco os sistemas que assistem ou determinam decisões em domínios especialmente sensíveis, como os do emprego — seleção, condições, promoção ou cessação da relação laboral —, acesso a serviços públicos essenciais incluindo a saúde, avaliação de risco de crédito, classificação de chamadas de emergência. Em todos estes casos, quem implementa o sistema deve informar os sujeitos



afetados de que estão sujeitas à sua utilização.

IV. Supervisão efetiva

O AI Act obriga quem implementa sistemas de alto risco a atribuir a supervisão humana a pessoas com competência, formação e autoridade, e a proporcionar-lhes o apoio para a exercerem. Não basta um formulário assinado ou um nome num organigrama.

Se a intervenção humana deve ser significativa, o verdadeiro debate não é se existe uma pessoa no circuito, mas se essa pessoa tem o poder, a capacidade, a competência e o tempo real para compreender o caso que tem pela sua frente e modificar o desfecho. O risco contemporâneo não é apenas que a máquina decida, mas que o ser humano se limite a validar por inércia aquilo que o algoritmo já concluiu. E uma validação sem compreensão não é supervisão.

Assim, a transparência não pode ser uma obrigação estética. O RGPD exige que nas decisões automatizadas sejam disponibilizadas informações úteis sobre a lógica subjacente, a importância e as consequências previstas.

Não se trata de revelar o algoritmo, mas de explicar

suficientemente o resultado para que a pessoa afetada o possa compreender, discutir e, se necessário, contestar.

V. A última fronteira

O RGPD traça uma linha de dignidade decisória: a automatização total em decisões que mudam vidas é a exceção, não a regra. E quando a IA atua nos domínios de alto risco, o AI Act exige que o ser humano não seja um espectador digital, mas um supervisor efetivo.

O ser humano não deverá ser a chancela que legitima a automatização, mas a última fronteira que separa a eficiência da despersonalização. O ponto em que a decisão volta a ser responsável, sindicável e, acima de tudo, humana. Porque a inteligência artificial pode calcular, prever e otimizar. Mas julgar — com tudo o que essa palavra implica — continua a ser, e deve continuar a ser, tarefa nossa.



Dados pessoais e interesse legítimo

Fundamentos de licitude para o treino de sistemas de IA



Augusto Almeida Correia

Director | Intellectual and Industrial Property

✉ augusto.correia@pt.Andersen.com

O debate em torno da inteligência artificial (IA) e da proteção de dados pessoais não é novo. O que é novo é a intenção da Comissão Europeia em reescrever algumas das regras fundamentais do Regulamento Geral sobre a Proteção de Dados (RGPD) através da proposta conhecida como Digital Omnibus. Dois dos temas mais sensíveis dessa proposta são os que este artigo visa abordar, a saber:

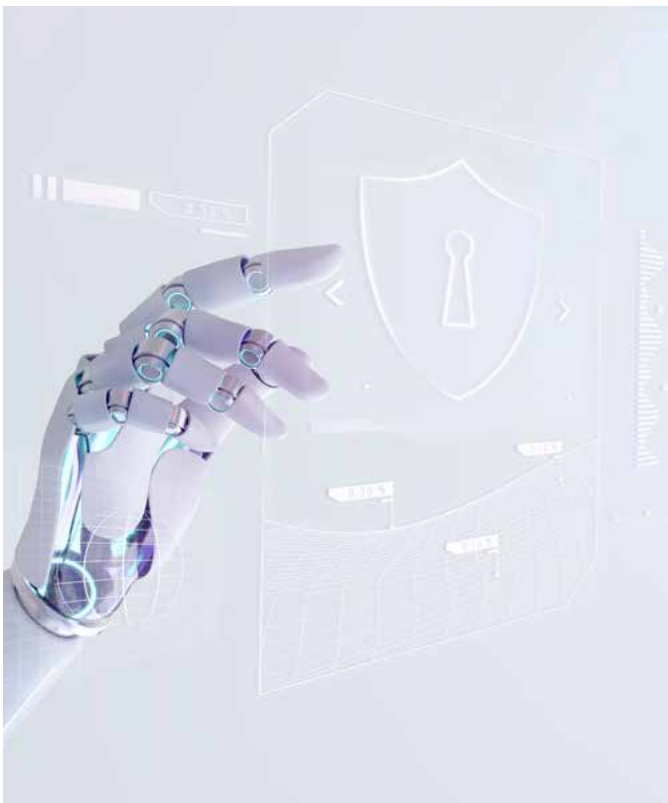
- ⚙ a clarificação do conceito de “dados pessoais”; e
- ⚙ a consagração expressa do interesse legítimo como base de licitude para o treino de sistemas de IA.



I. O conceito de dados pessoais

O RGPD define “dados pessoais” como informação relativa a uma pessoa singular identificada ou identificável, sendo considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial, por referência a um nome, número de identificação, dados de localização ou outros elementos específicos da sua identidade. Uma definição intencionalmente abrangente, pensada para proteger o cidadão independentemente do formato ou da sofisticação técnica do dado em causa.

Ora, o *Digital Omnibus* vem introduzir uma nuance de grande relevo: as informações relativas a uma pessoa singular não são necessariamente dados pessoais para qualquer entidade, mas apenas para aquela que disponha de meios razoavelmente suscetíveis de identificar o titular. Em linguagem simples, se uma empresa recebe dados codificados e não tem meios para os decodificar, esses dados podem não ser considerados “dados pessoais” para esta, ainda que outra entidade, com a chave certa, os identifique sem dificuldade.



A questão é saber se isto é compatível com a jurisprudência do Tribunal de Justiça da União Europeia, que sempre adotou uma interpretação ampla no sentido de a identificabilidade ser aferida tendo em conta todos os meios razoavelmente prováveis, incluindo por terceiros. Já a Autoridade de Controlo portuguesa, a Comissão Nacional de Proteção de Dados (CNPd), é clara ao recordar – aquando da sua pronúncia através do seu Parecer/2026/51 relativo ao projeto de Decreto-Lei que aprova o Regime Jurídico do Sistema Nacional de Ciência, Tecnologia e Inovação - que o tratamento de dados pessoais através de IA está sujeito ao RGPD ao longo de todo o ciclo de vida do sistema, sendo a definição relevante a do artigo 4.º, n.º 1, do RGPD. Este entendimento não deixa espaço para uma relativização excessiva do conceito.

Dito isto, o risco é real, ou seja, a nova redação proposta pode servir de fundamento a interpretações que esvaziem a proteção efetiva dos titulares, em especial nas cadeias de tratamento típicas do treino de modelos de IA, onde os dados transitam por múltiplas entidades antes de chegarem ao destino final.

II. O interesse legítimo não é um atalho

O RGPD prevê seis fundamentos que tornam lícito o tratamento de dados pessoais. O *Digital Omnibus* propõe consagrar expressamente um deles - o interesse legítimo - para o treino de sistemas e modelos de IA. O novo artigo 88.º-C do RGPD - introduzido pela proposta *Digital Omnibus* - prevê que, sempre que o tratamento seja necessário para o desenvolvimento e funcionamento de um sistema ou modelo de IA, pode ser prosseguido com esse fundamento, salvo se outra legislação exigir consentimento ou se prevalecerem os interesses ou direitos fundamentais do titular, em especial se for uma criança.



Em abstrato, a ideia tem o seu mérito, isto porque o treino, teste e validação de modelos de IA envolvem frequentemente dados pessoais, e dispor de uma base jurídica expressa traz segurança jurídica. Mas a consagração legislativa deste fundamento não significa que o seu recurso seja automático. O *European Data Protection Board* (EDPB) é claro: o interesse legítimo não deve ser tratado como uma base de recurso de último acesso, nem escolhido por ser percecionado como menos exigente. Assim, e para que o tratamento possa assentar neste fundamento, três condições cumulativas têm de estar preenchidas:

- ⚙ Existir um interesse legítimo genuíno;
- ⚙ O tratamento ser necessário para o prosseguir; e
- ⚙ Os interesses ou direitos fundamentais dos titulares dos dados não prevalecerem sobre esse interesse;

A CNPD adota o mesmo raciocínio, exigindo um teste de três etapas: identificar o interesse, que deve ser lícito, claro e real; verificar a necessidade, ponderando se existem meios menos intrusivos igualmente eficazes; e avaliar se esse interesse prevalece sobre os direitos do titular.



O interesse legítimo não dispensa o teste de necessidade e de ponderação."



É na segunda e terceira etapas que residem as questões mais delicadas. Pode o modelo ser treinado com dados sintéticos ou anonimizados? Se sim, o tratamento de dados pessoais pode simplesmente não ser necessário. E no teste de ponderação, a questão central é esta: alguém que publicou uma fotografia numa rede social, ou escreveu um artigo de opinião, esperava que esse conteúdo pudesse integrar um dataset de treino de um modelo de linguagem? As expectativas razoáveis do titular são um fator decisivo e em muitos casos, a resposta será negativa.

A própria proposta reconhece esta tensão, impondo que o responsável considere as expectativas razoáveis do titular, medidas técnicas para minimizar riscos como a fuga de dados, e um direito incondicional de oposição ao tratamento.

III. Uma salvaguarda que não deve ser ignorada

O novo artigo 88.º-C do RGPD - introduzido pela proposta *Digital Omnibus* - não se limita a abrir a porta ao interesse legítimo como fundamento para o treino de IA. Impõe também um conjunto de obrigações concretas a quem trate dados pessoais com esse fundamento, nomeadamente:

- ⚙️ selecionar as fontes de dados de forma criteriosa e restrita (minimização);
- ⚙️ proteger os dados que possam ter ficado retidos no sistema após o treino (dados residuais); e
- ⚙️ informar os titulares de forma clara sobre o que está a ser feito com os seus dados.

Após oposição, o responsável não pode continuar a tratar os dados a menos que demonstre razões imperiosas que prevaleçam sobre os interesses, direitos e liberdades do titular, sendo o ónus da prova do responsável pelo tratamento. Este direito de oposição incondicional é uma das poucas garantias concretas que a proposta assegura. E a sua eficácia dependerá, em grande medida, de os titulares saberem que podem exercê-lo, o que remete para o princípio da transparência, que o *Digital Omnibus* não reforça, antes procura, em outros contextos, atenuar.

IV. Entre a inovação e a proteção

O *Digital Omnibus* está ainda em fase de proposta sendo que o texto final poderá ser substancialmente diferente. Mas as orientações que estabelece revelam uma tensão que o legislador europeu ainda não resolveu: como viabilizar a inovação em IA sem comprometer a proteção efetiva dos direitos dos cidadãos.

A clarificação do conceito de dados pessoais e a consagração do interesse legítimo para o treino de IA podem trazer clareza. Mas clareza não é o mesmo que permissividade. O triplo teste acima mencionado continua a ser exigido, as expectativas razoáveis dos titulares continuam a ser o ponto central, e o direito de oposição continua a existir. O que mudará, se a proposta avançar, é que as empresas passam a ter uma base normativa mais explícita. Se isso se traduz em maior compliance ou em maior criatividade jurídica na invocação da norma, dependerá, como sempre, de quem fiscaliza e de quão seriamente o pretende fazer.





Impacto da NIS2 no setor da Saúde

Em particular nos Dispositivos Médicos e Ensaios Clínicos



Daniel Torres Gonçalves

Partner | Intellectual and Industrial Property

✉ daniel.goncalves@pt.Andersen.com

A Diretiva (UE) 2022/2555, conhecida como NIS2, vem colocar o setor da Saúde no centro de um novo paradigma regulatório em matéria de cibersegurança. Isto surge num momento em que o setor da Saúde enfrenta outras inovações regulatórias desafiantes – em particular ao nível dos dispositivos médicos e da Inteligência Artificial.

A NIS2 distingue entre entidades essenciais e entidades importantes, atribuindo ao setor da Saúde a qualificação de setor essencial. Isto significa que os operadores desta área vão assumir obrigações acrescidas em matéria de gestão de risco de cibersegurança, notificação de incidentes, continuidade de negócio e responsabilidade dos órgãos de administração.

Neste setor da Saúde vão estar incluídos os prestadores de cuidados de Saúde, como clínicas, hospitais e laboratórios, e também os operadores do ciclo de vida dos dispositivos médicos e atores que operam no âmbito da investigação clínica. O que motiva a inclusão destas entidades como obrigadas pela NIS2 prende-se com o facto de um ataque de cibersegurança a elas poder afetar a boa prestação de cuidados de Saúde, o que pode colocar em causa a Saúde e, até, a vida humana. A natureza dos dados tratados, como os registos clínicos, bem como o crescimento da quantidade de dados recolhidos, tornam o setor um alvo privilegiado e, simultaneamente, um domínio onde as consequências de uma falha poderão ser muito graves.



Como acontece com as demais áreas, a NIS2 irá impor um conjunto de medidas técnicas e organizativas obrigatórias, nas quais se podem incluir políticas de análise de risco e segurança dos sistemas, planos de gestão de incidentes e de continuidade de negócio, segurança na cadeia de abastecimento, medidas de controlo de acesso e criptografia e programas de formação em cibersegurança. Ao mesmo tempo, prevê-se a potencial responsabilização dos órgãos de administração.





I. O caso dos dispositivos médicos

No contexto dos dispositivos médicos, o impacto da NIS2 é de uma complexidade particular, porque se sobrepõe a um ambiente já densamente regulado. Em particular, refira-se o Regulamento (UE) 2017/745 (MDR), que estabelece os requisitos de segurança e desempenho dos dispositivos médicos, e o Regulamento (UE) 2024/1689 (Regulamento da IA), que impõe obrigações adicionais para os dispositivos que integrem sistemas de IA e que são, por definição, classificados como de alto risco. A NIS2 acrescenta uma nova camada, incidindo sobre a segurança das redes e sistemas de informação utilizados no contexto clínico.

Em particular, os dispositivos que apresentem conectividade com redes de informação, serão vulneráveis a ataques informáticos. Isto poderá suceder com um desfibrilador automático, um sistema de diagnóstico por imagem ou de monitorização remota, uma bomba de insulina que ajusta dosagens em tempo real. Sabendo que o MDR se centra na segurança clínica e no desempenho dos dispositivos médicos, não foi concebido para salvaguardar os riscos de cibersegurança, o que vem suceder com a NIS2.

A cadeia de abastecimento merece atenção especial. Os fabricantes de dispositivos médicos dependem frequentemente de fornecedores de software, módulos de IA e infraestruturas de armazenamento em nuvem. A NIS2 obriga-os a estender a sua análise de risco a toda essa cadeia. Note-se que o Regulamento da IA já impõe aos operadores de sistemas de alto risco que garantam a qualidade e integridade dos dados ao longo de todo o ciclo de vida do sistema. O mesmo raciocínio irá valer com a NIS2 aplicada aos dispositivos médicos.

II. O caso dos ensaios clínicos

Os ensaios clínicos representam um ponto particular de vulnerabilidade, que a NIS2 torna mais visível, ainda que não o faça de forma expressa. Neste domínio, o Regulamento (UE) 536/2014 constitui o quadro jurídico central, estabelecendo os requisitos para a condução de ensaios clínicos de medicamentos para uso humano. Mas os dados que circulam num ensaio clínico são, ao mesmo tempo, dados pessoais sensíveis e um ativo económico relevante.

A crescente utilização de IA nos ensaios clínicos intensifica este risco, nomeadamente com os algoritmos de seleção de participantes, os sistemas de monitorização e de análise de dados. Mais uma vez, a NIS2 pretende reforçar a segurança dos dados durante todo o circuito que eles fazem.

As entidades promotoras de ensaios clínicos e os parceiros tecnológicos serão forçadas a integrar nos seus protocolos de investigação uma análise de cibersegurança que considere os vários vetores de legislação aplicável, quer ao nível dos ensaios clínicos, da IA e da cibersegurança.





III. A conformidade regulatória para os operadores da Saúde

Os vários regimes que temos abordado, NIS2, Regulamento da IA e MDR, foram concebidos com objetivos que se complementam, mas sem uma arquitetura comum que os articule de forma coerente. O MDR centra-se na segurança clínica do produto. O Regulamento da IA centra-se na fiabilidade, transparência e supervisão humana dos sistemas inteligentes. A NIS2 centra-se na resiliência das infraestruturas digitais.

Para os operadores do setor da Saúde, a conformidade regulatória não será um exercício linear. Mostra-se necessário uma abordagem complementar, identificando-se as obrigações que se cumulam, as que se excluem e as que carecem de clarificação. A falta de orientações, bem como a carência de organismos notificados com capacidade para lidar com sistemas de IA, agrava esta incerteza.

A NIS2 vem afirmar-se como uma resposta a uma questão incontornável: o setor da Saúde é sistematicamente visado por ataques informáticos e por violações de dados. O impacto de um incidente grave pode ter consequências ao nível da Saúde e mesmo da vida humana.

Assim, a NIS2 pretende transformar a cibersegurança num conjunto de obrigações cujo cumprimento terá um impacto prático claro. Isto mostra-se particularmente relevante no setor da Saúde, considerando o tipo de dados que está em questão e o potencial impacto de uma falha nesta área. A confiança no sistema de Saúde também passará pela capacidade deste proteger os pacientes dos riscos da cibersegurança.

Num período marcado por exigências regulatórias de elevada complexidade, as entidades do setor da Saúde não poderão deixar de encarar a NIS2 como um desafio exigente, mas essencial para o futuro do setor.



IA e a prospeção de textos e dados

As novas exceções ao direito de autor na Europa



Gonçalo Gil Barreiros

Local Partner | Intellectual and Industrial Property

✉ goncalo.barreiros@pt.Andersen.com

A Inteligência Artificial trouxe ao domínio da Propriedade Intelectual, nomeadamente do direito de autor e direitos conexos, um conjunto de incertezas e desafios. A conjugação entre estes dois campos mostra-se fundamental para o mercado da União que se pretende competitivo e propício à inovação face aos demais concorrentes globais, como é o caso dos Estados Unidos da América e Ásia.

Por outro lado, há muito que se reclamava a necessidade de uma regulamentação europeia no âmbito do direito de autor e direitos conexos que se adaptasse, de forma efetiva, ao atual mundo digital em que vivemos.



I. A tensão entre o desenvolvimento de IA e a utilização de obras protegidas: a exceção de prospeção de textos e dados

A IA é uma realidade cada vez mais presente no quotidiano. Efetivamente, nos dias de hoje, para além de ser utilizada de forma generalizada (v.g. aplicações tecnológicas), mostra-se essencial para a investigação científica em diversas áreas de conhecimento e, de igual modo, no âmbito da criação de modelos de negócio.

Foi identificada, aliás, pela Comissão Europeia como se tratando de um vetor crítico e estratégico da Europa.

Ora, para que tais sistemas de IA se desenvolvam e melhorem a sua resposta, os mesmos necessitam de aceder e ser “alimentados” por inúmeras quantidades de conhecimento (textos e dados). Mas o acesso aos mesmos não se mostra suficiente, é necessário o recurso a técnicas para o tratamento desses dados, no fundo, o recurso à denominada técnica de prospeção de textos e dados (conhecida pela sigla inglesa TDM – *Text and Data Mining*, doravante designada de TDM).

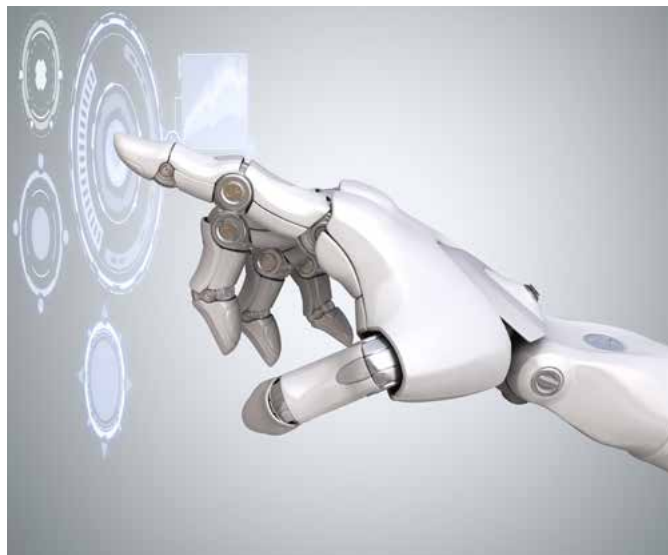


Contudo, a verdade é que tal aprendizagem automatizada se faz através da utilização massiva de obras que, na sua grande maioria, se mostram protegidas por direito de autor e direitos conexos, quer isso ocorra através de atos de reprodução de tais obras, quer através de atos de extração no caso de base de dados. Pois bem, para que tal utilização se mostrasse lícita, seria necessária a prévia autorização dos respetivos titulares de direitos e bem assim do pagamento, aos mesmos, de uma remuneração como contrapartida de tal autorização.

Deste modo, esta tensão conduziu, num primeiro momento, a Comissão Europeia e, num segundo momento, o Parlamento Europeu, aquando da discussão e aprovação da Diretiva 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 (doravante designada de DMUD), a que se tenha considerado justificável, por forma a não bloquear o desenvolvimento da IA na Europa, a introdução de uma nova exceção ao direito de autor relativamente quer à prospeção de textos e dados para fins de investigação científica por parte de organismos de investigação e entidades responsáveis pelo património cultural, quer para outros fins.

II. A prospeção de textos e dados para fins de investigação científica

De acordo com a DMUD (art. 2º.2), por prospeção de textos e dados entende-se *“qualquer técnica de análise automática destinada à análise de textos e dados em formato digital, a fim de produzir informações, tais como padrões, tendências e correlações entre outros”*. Tratando-se de uma nova forma de utilização trazida pelas tecnologias digitais, trata-se de uma ferramenta que *“torna possível o tratamento de grandes quantidades de informação para obter novos conhecimentos e descobrir novas tendências”* (Considerando 8 da DMUD), beneficiando a comunidade científica e a inovação, sendo predominantes na economia digital.



Ora, a insegurança jurídica com que eram confrontadas as universidades e organismos de investigação, bem como instituições responsáveis pelo património cultural, sobre até onde podiam ir na prospeção de textos e dados de conteúdos digitais (por poder colidir com direitos de autor ou com o direito sui generis sobre bases de dados), fez com que o legislador europeu estabelecesse uma exceção obrigatória, com a exclusão de admissibilidade de convenção em contrário e/ou proteção técnica que a impeça, prevalecendo sobre eventuais condições de assinatura de publicações ou de termos de licenças de acesso aberto que excluam a TDM para fins de investigação científica, mas apenas admissível para tais instituições e organizações (especificadamente definidas nos artigos 1º.1 e 3 da DMUD). Sendo limitada a atos de reprodução e extração de base de dados depende, contudo, dos beneficiários, da mesma, terem acesso aos conteúdos protegidos de forma legal.

Deste modo, não carecem, assim, de autorização do titular de direitos as *“reproduções e extrações efetuadas por organismos de investigação e por instituições responsáveis pelo património cultural para a realização de prospeção de textos e dados de obras ou outro material protegido a que tenham acesso legal para efeitos de investigação científica”* (art. 3º.1 da DMUD).

A exceção instituída permite também o armazenamento de cópias de obras ou outro material protegido desde que ocorra com um nível de segurança adequado e em ambiente seguro para tais fins de investigação científica e verificação posterior dos resultados de tal investigação. Os próprios titulares poderão aplicar tais medidas, todavia, sempre no âmbito do necessário para o efeito, não devendo as mesmas restringir quer a aplicação da exceção, quer outras utilizações para aqueles fins de investigação como sendo a revisão científica de pares e a investigação conjunta.



III. A prospeção de textos e dados para outros fins

Para além da importância da TDM no contexto de investigação científica, tais técnicas são “*amplamente utilizadas*” para outros fins, como sendo em decisões empresariais complexas e para o desenvolvimento de novas aplicações ou tecnologias.

Nesse sentido, para proporcionar maior segurança jurídica e “incentivar a inovação também no sector privado” (Considerando 18 da DMUD), estabeleceu o legislador europeu uma exceção geral supletiva para as reproduções e as extrações de obras e de outro material protegido, legalmente acessíveis (como as disponibilizadas em linha ao público), para fins de prospeção de textos e dados, aplicável no âmbito dos direitos sobre bases de dados, programas de computador e direito do editor de publicações de imprensa. Contudo, os titulares de direitos podem

reservar o TDM e assim impedir a prospeção de textos e dados para fins diversos da investigação científica, mediante a utilização de meios de leitura ótica (v.g. metadados, ficheiros robots.txt ou definição de condições gerais num website ou serviço digital) quanto a conteúdos disponibilizados em linha ao público, através de acordos contratuais, entre outros.

Efetivamente, tal reserva por parte dos titulares de direitos à reprodução e extração de obras em ambiente digital para efeitos de TDM tem apresentado uma aplicação prática relevante no âmbito e defesa do novo direito conexo na esfera do editor de publicações de imprensa (art. 15º da DMUD) quanto à utilização em linha das suas publicações (v.g. jornais e revistas), nomeadamente perante utilizações (como seja impedir que sejam livremente utilizados para treinar modelos de linguagem), por parte de prestadores de serviços da sociedade da informação.

IV. A transposição portuguesa da exceção de prospeção de textos e dados

A DMUD foi transposta para o ordenamento jurídico português pelo Decreto-Lei 47/2023, de 19 de junho, nos termos da qual “em face das possíveis opções legislativas quanto ao método a seguir na transposição da diretiva, é opção consciente seguir-se uma lógica de elevada proximidade com o texto original, permitindo que se encete o caminho jurisprudencial que a mesma terá de fazer”. Assim e no que respeita às exceções de TDM foram introduzidas as alíneas v) e w) no art. 75º.2 do Código do Direito de Autor e dos Direitos Conexos – doravante CDADC - (utilizações livres), com a previsão das noções de “organismo de investigação” e “prospeção de textos e dados”, no novo número 6 daquele artigo. De igual modo, introduziu o legislador nacional no art. 76º do CDADC, novos números 4 e 5 a propósito dos requisitos de tais utilizações livres.

Foram, igualmente, alterados os artigos 10º e 15º do Decreto-Lei 122/2000, de 04 de julho (relativo à proteção jurídica de bases de dados), por forma a permitir atos de reprodução e extração para a realização de TDM.



V. Conclusão

A consagração destas exceções representou, na Europa, um passo relevante na tentativa de equilibrar por um lado a proteção da propriedade intelectual e por outro o progresso tecnológico.

Atualmente este regime da DMUD funciona em complementaridade direta com o Regulamento da IA da União Europeia (*AI Act*).

Muito se discutiu e discute se a exceção de TDM introduzida na DMUD, e justificada pela necessidade de desenvolvimento de IA, não será, tal como foi configurada naquela, ainda um entrave significativo à evolução dos sistemas de IA europeus em comparação com demais sistemas, nomeadamente o norte-americano, mais permissivos (em que, recorrendo a uma cláusula de *fair use*, remete para os tribunais a definição dos limites entre o respeito pelos direitos de autor e o progressivo desenvolvimento tecnológico).

Contudo, uma coisa é certa, por muito que o desenvolvimento da IA se mostre fundamental para tornar o mercado europeu mais competitivo e inovador face à concorrência, a Europa não deverá adotar sistemas de flexibilidade quanto às políticas de desenvolvimento da IA que culminem na desvalorização de potenciais violações de direito de autor por parte dos utilizadores de tais sistemas e consequentemente na simples atribuição de todas as responsabilidades à máquina.



O progresso tecnológico será sustentável se caminhar lado a lado com a proteção do direito de autor.”





Andersen Global is a Swiss verein comprised of legally separate, independent member firms located throughout the world providing services under their own names. Andersen Global does not provide any services and has no responsibility for any actions of the Member Firms or collaborating firms. No warranty or representation, express or implied, is made by Andersen Global, its Member Firms or collaborating firms, nor do they accept any liability with respect to the information set forth herein. Distribution hereof does not constitute legal, tax, accounting, investment or other professional advice.