# AI ACT: ALINHAR A INOVAÇÃO À CIBERSEGURANÇA

Foto de Andrea De Santis na Unsplash

POR RITA SOUSA E SILVA

A LEI DE IA DA UNIÃO EUROPEIA ENFRENTA O DESAFIO DE ASSEGURAR A SEGURANÇA SEM CORTAR AS PERNAS DA INOVAÇÃO. À MEDIDA QUE OS CIBERCRIMINOSOS APERFEIÇOAM A SUA ATIVIDADE COM A TECNOLOGIA, COLOCAR A CIBERSEGURANÇA NO CENTRO DA REGULAÇÃO DA IA TORNA-SE CADA VEZ MAIS IMPORTANTE.

Regular a Inteligência Artificial (IA) é uma corrida contra o tempo: quanto mais a elaboração de um enquadramento regulatório demora, mais rápido a tecnologia inovadora avança e mais alarmantes são as preocupações ligadas à segurança, privacidade e proteção de dados. Enquanto isso, os cibercriminosos – com menor ou maior experiência – aproveitam-se da facilidade de utilização da IA para realizar ataques cada vez mais sofisticados.

A União Europeia (UE) lançou a primeira pedra na regulamentação da IA, centrando-se sobretudo na mitigação dos riscos – e a cibersegurança é inegavelmente um deles. "Qualquer regulação de IA vai ter de olhar também para o tema da cibersegurança", afirma Eduardo Magrani, Consultor Sénior da área de Tecnologias, Media e Telecomunicações da CCA Law Firm.

Margarida Leitão Nogueira, Partner da DLA Piper, relembra a dicotomia inerente à IA em matéria de segurança cibernética. Por um lado, "a IA é suscetível de ter um papel essencial no que respeita ao reforço da cibersegurança das organizações e no combate ao cibercrime" e, por outro, "pode potenciar a sofisticação e disseminação de ciberataques, se utilizada com propósito malicioso".

Os legisladores europeus enfrentam um desafio crucial na produção da legislação pioneira sobre a IA: garantir a segurança digital sem travar a evolução tecnológica e a competitividade no espaço europeu.

## LUZ VERDE DO PARLAMENTO

Em junho, o Parlamento Europeu deu luz verde à proposta do AI Act, assente nos princípios de segurança, privacidade e transparência. As regras seguem uma abordagem baseada no risco, estabelecendo obrigações para fornecedores e utilizadores de sistemas de IA.

"Não existe segurança garantida nas TIC, incluindo nos sistemas de IA", destaca a Agência Europeia

para a Segurança das Redes e da Informação (ENISA). "No entanto, uma avaliação de riscos permite tomar uma decisão informada sobre quais são as possíveis ameaças e vulnerabilidades e como minimizar o seu impacto".

O projeto de lei incide sobre os sistemas de IA classificados como sendo de risco inaceitável, que são considerados "uma ameaça para as pessoas" e, por isso, será proibida a sua utilização, assim como a sua colocação no mercado ou em serviço. Estes incluem a manipulação cognitivo-comportamental de pessoas ou grupos vulneráveis específicos, a pontuação social e os sistemas de identificação biométrica em tempo real e à distância.

Por sua vez, os sistemas de IA de risco elevado estão "sujeitos a requisitos exigentes por serem suscetíveis de colocar em causa a segurança ou direitos fundamentais", explica Margarida Leitão Nogueira. Estes dividem-se em duas categorias: aqueles que são utilizados em produtos abrangidos pela legislação da UE em matéria de segurança dos produtos; e aqueles que estão enquadrados em determinadas


EDUARDO MAGRANI, CCA LAW FIRM

áreas específicas que terão de ser registados numa base de dados da UE.

As tecnologias de alto risco "têm medidas muito específicas: garantia de explicabilidade dos algoritmos; maior transparência aos utilizadores; necessidades de auditorias, de relatórios de impacto", afirma Eduardo Magrani. Os utilizadores deverão receber das organizações que recorrem à tecnologia "informações mais detalhadas sobre que tipo de IA ou de algoritmo é aplicado, quais são os riscos atrelados,

> AS TECNOLOGIAS DE ALTO RISCO "TÊM MEDIDAS MUITO ESPECÍFICAS: GARANTIA DE EXPLICABILIDADE DOS ALGORITMOS; MAIOR TRANSPARÊNCIA AOS UTILIZADORES; NECESSIDADES DE AUDITORIAS, DE RELATÓRIOS DE IMPACTO",
>
> EDUARDO MAGRANI, CONSULTOR SÉNIOR DA ÁREA DE TECNOLOGIAS, MEDIA E TELECOMUNICAÇÕES DA CCA LAW FIRM

como é que controlam esses riscos". O advogado acrescenta que "as autoridades vão ser mais munidas com essas informações, então os utilizadores vão sentir-se mais empoderados para reivindicar os seus direitos".

A ENISA destaca o artigo 15.º da Lei da IA, que "propõe requisitos de cibersegurança para sistemas de IA de alto risco, a fim de garantir o *compliance*, identificar riscos e implementar as medidas de segurança necessárias". Neste sentido, "uma avaliação de risco de segurança deve ser realizada tendo em conta a conceção do sistema e a finalidade a que se destina".

Para Margarida Leitão Nogueira, "um dos aspetos relevantes constantes" do AI Act é a "garantia de solidez técnica e de resistência a ações maliciosas suscetíveis de pôr em causa a segurança dos sistemas de IA de risco elevado". Neste sentido, a proposta estabelece "que 'os sistemas de IA de risco elevado devem ser concebidos e desenvolvidos de acordo com o princípio da segurança desde a conceção e por defeito', devendo atingir um nível apropriado de cibersegurança durante o ciclo de vida".

Além disto, os responsáveis pela implementação dos sistemas de IA de risco elevado "estão obrigados a garantir a monitorização regular da eficácia das medidas de solidez e cibersegurança, bem como a respetiva atualização", acrescenta a advogada.

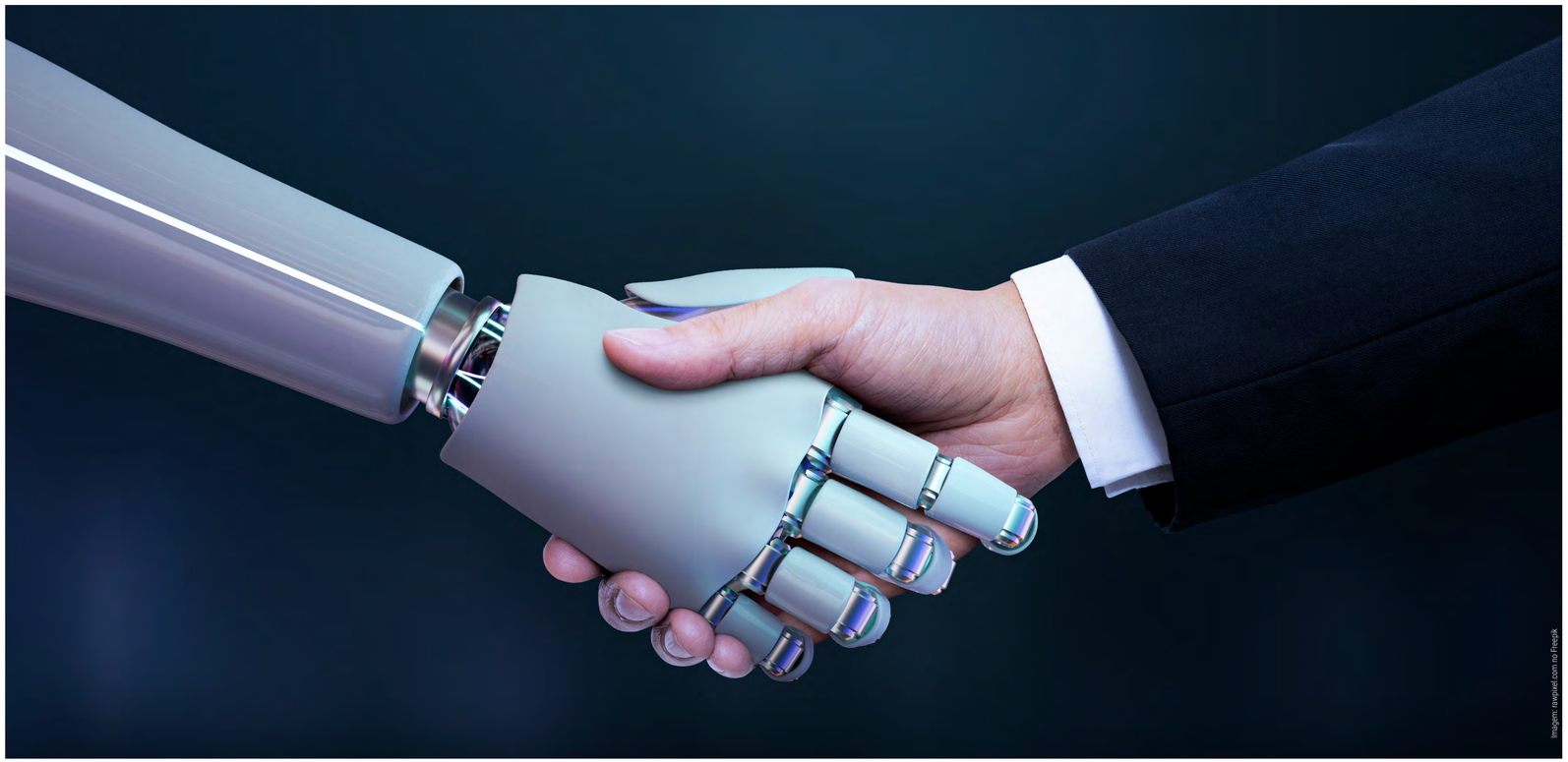
Já os sistemas de IA de risco limitado deverão cumprir requisitos mínimos de transparência de forma que os utilizadores tomem decisões informadas sobre a sua utilização.

Com a aprovação do Parlamento Europeu, os eurodeputados decidiram alargar a lista de proibições para incluir "utilizações intrusivas e discriminatórias da IA", como é o caso dos sistemas de identificação biométrica à distância, tanto em tempo real em espaços públicos como em diferido, e dos sistemas de categorização biométrica que utilizem características sensíveis (como género, raça, etnia, estatuto de cidadania, religião, orientação política).

São também proibidas as utilizações de sistemas de policiamento preditivo, bem como de reconhecimento de emoções na aplicação da lei, gestão das fronteiras, local de trabalho e nos estabelecimentos de ensino. Os eurodeputados classificam também como risco inaceitável a remoção não direcionada de imagens faciais da Internet ou de filmagens de videovigilância para criar bases de dados de reconhecimento facial.

Além disto, os fornecedores de modelos de base estarão incumbidos de avaliar e mitigar eventuais riscos, devendo registar estes modelos na base de dados da UE. Os sistemas de IA generativa que têm por base estes modelos, como o ChatGPT, terão de cumprir os requisitos de transparência com, por exemplo, a disponibilização aos utilizadores de resumos pormenorizados dos dados protegidos por direitos de autor.

"O ponto mais importante é entender que [o AI Act] não está sozinho", reforça Eduardo Magrani. Regulações como o RGPD, a NIS 2, o DORA e frameworks de segurança como o ISO e o NIST, refe-




re, "são complementares às determinações do AI Act e não podem ser esquecidas na fase de implementação, lembrando que essas entidades não têm de esperar o dano ocorrido".

## ARMA DE CIBERCRIMINOSOS

Devido à sua fácil utilização, os cibercriminosos têm usufruído dos vários benefícios da IA – nomeadamente a capacitação de um maior número de utilizadores, incluindo os menos experientes – para realizar atividades maliciosas. As ferramentas de IA "podem fornecer análises melhores e mais rápidas dos sistemas investigados, ser usados em ataques de engenharia social ou apoiar a criação de malware personalizado", explica a ENISA.

De acordo com a Check Point, isto levou à criação de pequenos grupos de cibercriminosos capazes de encetar ciberataques mais sofisticados devido a esta tecnologia.

Os *deepfakes*, uma ferramenta de IA que possibilita a criação de gravações de voz e de vídeo falsas/manipuladas, são frequentemente utilizados para os atacantes se fazerem passar por celebridades, líderes políticos ou executivos de organizações.

Os grupos de ransomware estão a desenvolver novos métodos em que combinam a IA com ferramentas há muito estabelecidas, como dispositivos USB, para realizar ciberataques disruptivos, alerta a Check Point.

Em março, a Europol, a Agência da UE para a Cooperação Policial, alertou para o potencial uso indevido de ferramentas como o ChatGPT em três áreas específicas: os ataques de phishing, devido à sua capacidade de "redigir textos altamente realistas"; os cibercrimes, uma vez que os atacantes podem aproveitar-se da habilidade de "reproduzir padrões de linguagem para personificar o estilo de fala de indivíduos ou grupos específicos"; e a desinformação.

Com as mensagens de phishing aperfeiçoadas,

"UM DOS ASPETOS RELEVANTES CONSTANTES" DO IA ACT É A "GARANTIA DE SOLIDEZ TÉCNICA E DE RESISTÊNCIA A AÇÕES MALICIOSAS SUSCETÍVEIS DE PÔR EM CAUSA A SEGURANÇA DOS SISTEMAS DE IA DE RISCO ELEVADO".

MARGARIDA LEITÃO NOGUEIRA, PARTNER DA DLA PIPER

é cada vez mais difícil distingui-las de comunicações legítimas. Todos os dias, as marcas de empresas como a Amazon, a Microsoft e a Google são utilizadas para o furto de dados através de emails e SMS fraudulentos, destaca a Check Point.

"À medida que as capacidades dos LLM, como o ChatGPT, estão a ser ativamente melhoradas, a exploração potencial destes tipos de sistemas de IA por criminosos oferece uma perspetiva sombria", adverte a Europol. "Para um potencial criminoso com pouco conhecimento técnico, este é um recurso inestimável para produzir código malicioso".

## INOVAÇÃO, COMPETITIVIDADE E SOBERANIA

Uma das maiores críticas ao AI Act é o entrave à inovação e a falta de competitividade. Recentemente, as maiores empresas da Europa – como a Siemens, Heineken, Renault e Airbus – manifestaram-se contra a regulação proposta pela UE, considerando que "comprometeria a competitividade e a soberania tecnológica da Europa sem efetivamente endereçar os desafios que estamos e estaremos a enfrentar".


MARGARIDA LEITÃO NOGUEIRA, DLA PIPER

"A Europa não se pode dar ao luxo de ficar à margem", reitera a carta aberta assinada por 163 executivos. Em vez de concentrar a regulação na IA generativa e implementar um "*compliance* rígido", os reguladores deveriam produzir uma lei que se limitasse aos "princípios amplos numa abordagem baseada em riscos", defendem.

Margarida Leitão Nogueira esclarece que as empresas europeias consideram a proposta "demasiado restritiva", podendo colocá-las "numa posição

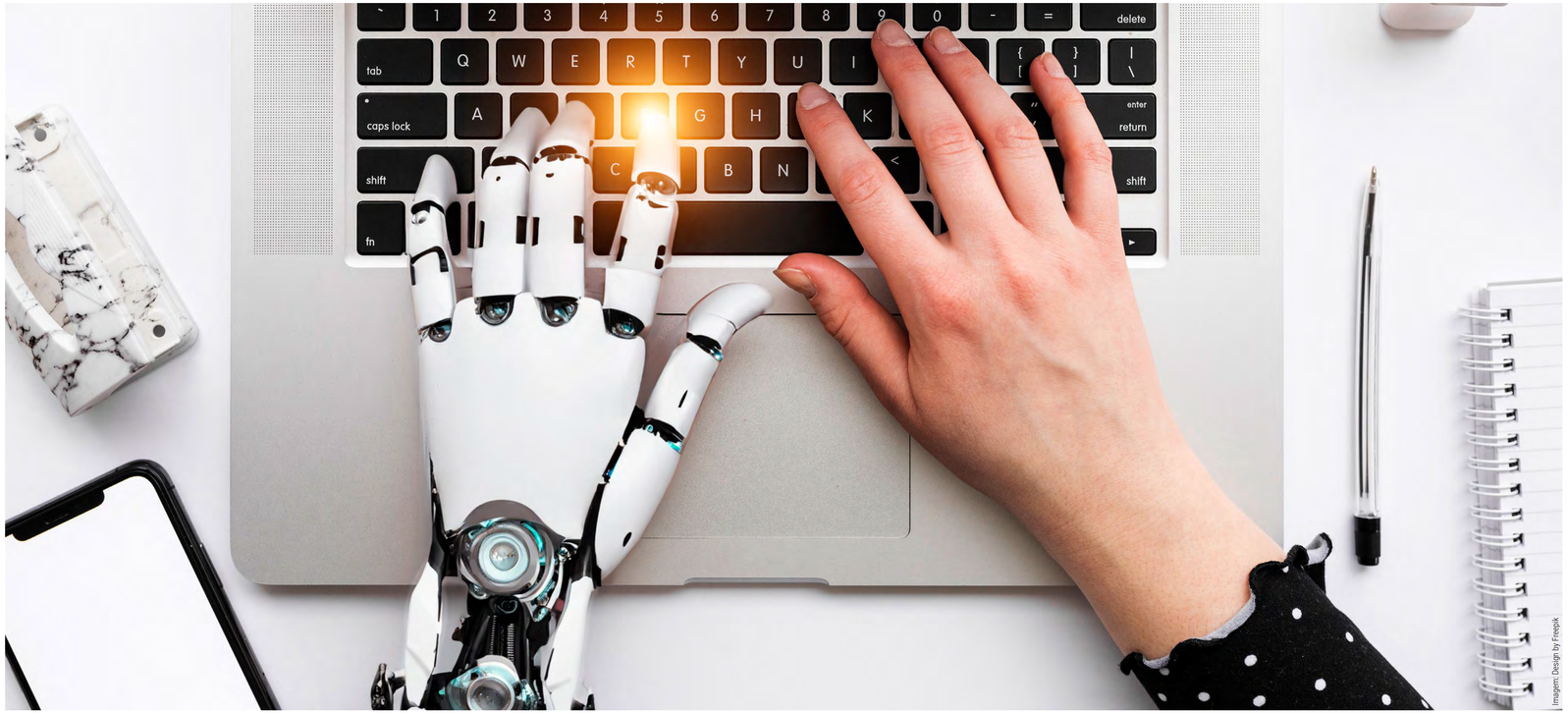


Imagem: Design by Freepik

de desvantagem, sobretudo face a concorrentes localizados nos Estados Unidos e China". Desta forma, é "determinante" a adoção de "soluções equilibradas e proporcionais de forma a não limitar a capacidade de inovação".

A questão da soberania tecnológica está "na ordem do dia", sendo que os ataques cibernéticos no conflito Ucrânia-Rússia "chamaram a atenção para o tema da cibersegurança ainda mais", segundo Eduardo Magrani. "Hoje, temos sistemas de *cloud computing* que não garantem uma hegemonia dos países e do bloco europeu que dependem da tecnologia de outras regiões", acrescenta. "Países como Alemanha e França vêm-se preocupando fortemente em como garantir a sua soberania digital em computação em nuvem".

Também os Estados Unidos alertaram que a proposta da UE prejudicará as pequenas empresas europeias, beneficiando somente as grandes organizações capazes de cobrir os elevados custos de compliance. O país acredita que o regulamento poderá ter consequências como a redução de produtividade e o desincentivo ao investimento.

O AI Act "terá um impacto económico e operacional significativo para as organizações", refere Margarida Leitão Nogueira, implicando "um maior esforço para pequenas empresas que não dispõe do mesmo nível de recursos financeiros e humanos". No entanto, o projeto de lei "prevê a necessidade de prestar particular atenção à redução dos encargos administrativos e dos custos de conformidade para as micro e pequenas empresas".

Eduardo Magrani sublinha a existência de um "*clash* geopolítico" sobre esta questão, uma vez que "os Estados Unidos têm uma abordagem muito mais afeita a riscos que a UE muitas vezes não está disposta", preferindo uma "legislação robusta, que crie mitigadores efetivos de risco antes de um produto ser colocado no mercado".

## PRINCIPAIS DESAFIOS

Em outubro, a Reuters reportou a dificuldade dos legisladores europeus na chegada a acordo sobre o projeto de lei. Em particular, a falta de consenso tem incidido sobretudo a abordagem aos "modelos de base", refere Margarida Leitão Nogueira, considerada "demasiado restritiva" por alguns países europeus.

"Tínhamos um texto muito maduro já no início desse ano, mas foi atrasado por conta do impacto da IA generativa", afirma Eduardo Magrani. "A introdução no mercado de uma plataforma como o ChatGPT foi altamente disruptiva".

No final de novembro, a Alemanha, França e Itália chegaram a um acordo sobre a forma como a IA deve ser regulamentada, o que deverá acelerar as negociações a nível europeu. Num documento conjunto, os três países apoiaram a "autorregulação obrigatória através de códigos de conduta" para os modelos básicos de IA, mas opõem-se às "normas não testadas".

"Juntos sublinhamos que a Lei da IA regula a aplicação da IA e não a tecnologia como tal", escreveram no documento. "Os riscos inerentes residem na aplicação de sistemas de IA e não na própria tecnologia".

As três potências europeias afirmaram que a Europa precisa de um "quadro regulamentar que promova a inovação e a concorrência, para que os intervenientes europeus possam emergir e transmitir a nossa voz e os nossos valores na corrida global da IA", segundo escreve o POLITICO.

Prevê-se que o AI Act entrará em vigor no final de 2025 ou no início de 2026. Devido ao "rápido desenvolvimento tecnológico" e "ao cenário de ameaças cibernéticas em constante mudança", os estados-membros "poderão enfrentar desafios na implementação da lei", acredita a ENISA.

"Se, em termos gerais, o cumprimento dos requisitos legais em matéria de cibersegurança coloca, por si só, desafios às organizações, tais desafios são de complexidade acrescida no contexto da IA, face às respetivas especificidades e vulnerabilidades", refere Margarida Leitão Nogueira.

Um dos principais desafios, segundo Eduardo Magrani, é a necessidade de "uma mudança cultural" no seio das organizações, uma vez que a regulação trará "um nível de compliance muito alto e nem todas as entidades estão preparadas". Desta forma, é necessário "começar a trilhar a jornada do compliance em proteção de dados, em cibersegurança, em ética de IA".

Uma preparação adequada, ainda antes da aprovação da regulação, poderá ser chave para o cumprimento bem-sucedido das medidas legais aplicáveis. Desta forma, Margarida Leitão Nogueira indica um conjunto de medidas transversais que poderão ser adotadas pelas organizações: "definir um modelo de governo, políticas e procedimentos internos claros em matéria de IA; sensibilizar para uma utilização responsável dos referidos sistemas; criar canais de comunicação eficazes; definir equipas multidisciplinares capazes de monitorizar a conformidade legal dos IA". ◀