TECH

LEADING

TECH

LEADING

TECH

LEADING TECH

TECH LEADING TECH

LEADING TECH

SPONSORED BY

visionware

NÚMEROS

Espera-se que a Inteligência Artificial contribua com
14,5 MIL MILHÕES DE EUROS
para a economia global até 2030.

Fonte: CompTIA, 2022.

As redes sociais influenciam
71% DAS DECISÕES DE COMPRA
dos consumidores.

Fonte: Search Engine Watch, 2020.

95% DAS QUEBRAS DE CIBERSEGURANÇA
são causadas por erro humano.

Fonte: World Economic Forum, 2022.

64% DOS NEGÓCIOS
esperam que a Inteligência Artificial aumente a produtividade.

Fonte: Forbes, 2023.

90% DOS DADOS
do Mundo foram gerados entre 2019 e 2022.

Fonte: CompTIA, 2022.

LETRAS

O FUTURO DO SANGUE não é apenas um avanço científico, mas significa também a criação de uma sociedade mais igualitária e justa.

Marco Espinheira, Diretor Executivo de Angariação de Fundos e Responsável de Corporate Relations e Public Affairs, na Nova SBE

Duvido que daqui a 20 anos não nos recordemos de que, aos 83 anos, Yvon Chouinard, Fundador da Patagonia, tenha decidido doar a empresa a um fundo solidário para combater a **CRISE CLIMÁTICA.**

Diana Carvalhido, Partner e Diretora Criativa na Ivity

Somos afortunados por vivermos todos naquela que pode ser a maior revolução da história da Humanidade de sempre, a entrada na **ERA DA INTELIGÊNCIA.**

Gonçalo Perdigão, Partner e Diretor-Geral da Algorithm G

O DESAFIO DE REGULAMENTAR A UTILIZAÇÃO DA INTELIGÊNCIA ARTIFICIAL

Rita Rugeroni Saldanha

Nova Lei será a primeira no Mundo e está a ser desenvolvida pela União Europeia.

Enviesamento, privacidade e segurança. Autonomia e controlo. Transparência e desemprego. A Inteligência Artificial, o seu uso e inevitável presença na vida das pessoas, empresas e sociedades, traz consigo inúmeras questões para as quais ainda não há respostas definitivas, nem concretas.

Existe, sim, a noção de que há efeitos nocivos e é necessária uma regulamentação na forma como se conduz o seu desenvolvimento e um tipo de abordagem ética para que os avanços tecnológicos sejam, no final de contas, pelo bem da Humanidade. Como fazer essas regras, que padrões éticos devem ser instituídos para que a comunidade global os deva seguir? Assim como um Código da Estrada em que, mesmo no meio de um deserto, em qualquer parte do Mundo, se virmos um sinal Stop paramos.

Assumindo que a partir do momento em que existe uma relação, entre dois humanos, ou, neste caso, humano-máquina, existe a noção de ética e da necessidade de se ser capaz de responder ao que a situação nos pede. Se os sistemas operacionalizados pela IA podem tomar decisões morais, como devem ser programados para o fazer? Como se deve posicionar o Homem perante a máquina e que padrões de conduta devem existir na forma como a utiliza?

E ainda há que pensar sobre a concentração de poder das grandes tecnológicas na vanguarda do desenvolvimento de IA, cujo controlo fica nas mãos de uns *happy few* mas o potencial para a sua utilização em fins menos éticos, e maliciosos, está ao alcance de muitos.

União Europeia desenvolve pela primeira vez uma lei sobre IA

Em junho deste ano, os eurodeputados negociaram a sua posição sobre o Regulamento de Inteligência Artificial (IA), cujas regras, uma vez aprovadas, serão as primeiras do Mundo sobre a matéria. Até ao final do ano está previsto chegar-se a um acordo, cujo esboço será parte da Lei da UE sobre IA.

Composta por princípios que promovem a adoção de uma IA centrada no ser humano e fiável, as regras procuram proteger a saúde, a segurança, os direitos fundamentais e a Democracia.

Propõe-se que os sistemas de IA utiliza-

dos em diferentes setores sejam analisados e classificados de acordo com o risco que representam para os utilizadores. Os diferentes níveis de risco vão depois implicar maior ou menor regulamentação.

Segundo informação partilhada pelo Parlamento Europeu, a prioridade é garantir que os sistemas sejam «seguros, transparentes, rastreáveis, não discriminatórios e respeitadores do ambiente». E acrescenta ainda que «devem ser supervisionados por pessoas, em vez de serem automatizados, para evitar resultados prejudiciais».

Haverá também regras diferentes para diferentes tipos de risco. Ou seja, as novas regras tencionam estabelecer obrigações para os fornecedores e utilizadores em função do nível de risco dos sistemas de IA.

Risco inaceitável

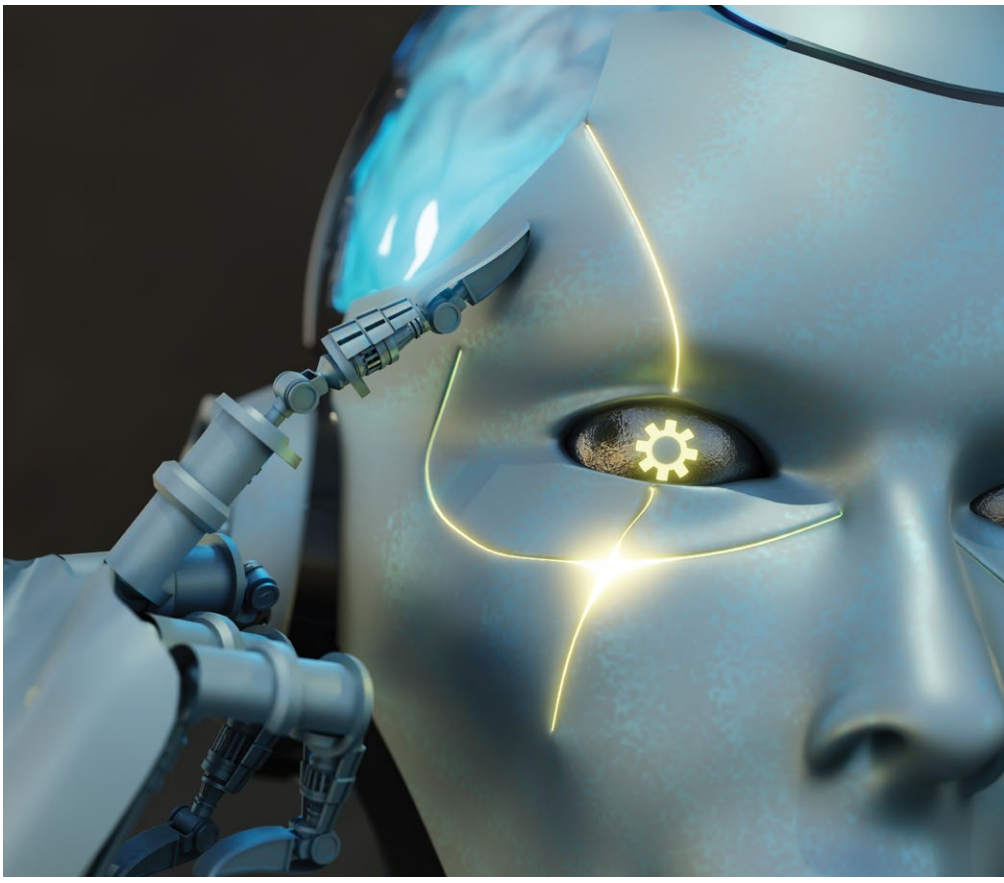
Os sistemas de risco inaceitável são sistemas considerados uma ameaça para as pessoas e serão proibidos. Estes sistemas incluem a manipulação cognitivo-comportamental de pessoas ou grupos vulneráveis específicos, como por exemplo, brinquedos ativados por voz que incentivam comportamentos perigosos nas crianças; casos de pontuação social, isto é, classificação de pessoas com base no comportamento, estatuto socioeconómico e caraterísticas pessoais e os sistemas de identificação biométrica em tempo real e à distância, como o reconhecimento facial.

Risco elevado

Os sistemas de risco elevado são os que afetam negativamente a segurança ou os direitos fundamentais, divididos em duas categorias:

1. Sistemas que são utilizados em produtos abrangidos pela legislação da UE em matéria de segurança. Isto inclui brinquedos, aviação, automóveis, dispositivos médicos e elevadores;

2. Sistemas que se enquadram em oito áreas específicas que devem ser registados numa base de dados da UE: identificação biométrica e categorização de pessoas singulares; gestão e funcionamento de infraestruturas essenciais; educação e formação profissional; emprego, gestão dos trabalhadores e acesso ao trabalho por conta própria; acesso e usufruto de serviços privados essenciais e de serviços e benefícios públicos; aplicação da lei; gestão da migração, do asilo e do controlo das fronteiras e assistência na interpretação jurídica e na aplicação da lei.



Risco limitado – a Inteligência Artificial Generativa

Também a nova Lei sobre IA considera um capítulo dedicado à IA Generativa, que terá requisitos de transparência, tais como divulgar a origem do conteúdo e conceber o modelo de forma a evitar que produza conteúdos ilegais.

A IA generativa é um termo usado para qualquer tipo de processo automatizado que utiliza algoritmos para produzir, manipular ou sintetizar dados, muitas vezes sob a forma de imagens ou texto. É dita «generativa» porque cria algo que não existia anteriormente. Na sua versão mais popular estão os LLM (Large Language Models) como o ChatGPT e DALL-E.

Segundo o novo projeto de Lei, no que se refere a sistemas de risco limitado, os mesmos devem cumprir requisitos mínimos de transparência que permitam aos utilizadores tomar decisões informadas. Depois de interagir com as aplicações, tendo sido devidamente alertado para isso, o utilizador pode decidir se quer continuar a utilizá-las. Isto diz respeito também aos sistemas de IA que geram ou manipulam conteúdos de imagem, audio ou vídeo (por exemplo, os *deepfakes*).

Bruno Castro
Fundador & CEO da VisionWare

O QUE FAZER PARA PREVENIR O FUTURO?

Manter a desconfiança costuma ser, habitualmente, o melhor caminho a seguir para garantirmos uma maior segurança quando navegamos na Internet e nas nossas redes sociais. Tal como em qualquer esquema fraudulento, devemos manter-nos sempre atentos, preventivos, e sobretudo, não clicar em *links* cujas origens não conhecemos ou poderão ser de índole duvidosa e/ ou criminosa. Por norma, devemos desconfiar, sempre.

Os ciberataques de *ransomware* continuam em ascensão, afetando transversalmente todas as áreas de atividade. Devido ao incremento (e manutenção) do trabalho remoto, motivado e acelerado pela pandemia, estima-se que estes ataques tenham aumentado 148% em todo o Mundo. O *ransomware* constitui, por isso, uma ameaça visível para milhares de organizações e empresas, inclusive em Portugal, que, quando comparada com a tendência noutros países europeus, e de acordo com dados recolhidos pelo Tech Monitor, surge a ocupar o 3.º lugar com uma incidência de 9% no que toca aos ciberataques registados em toda a Europa no ano 2022. Os protagonistas deste tipo de ciberataques sabem que o seu modelo de negócio, altamente destrutivo, terá garantia de sucesso contínuo, desde que consigam inovar as suas técnicas de exploração e formatos de dispersão dentro da organização.

Há que fazer mais e melhor para prevenir o futuro, já que as implicações e consequências para qualquer empresa e marca podem ser devastadoras (incluindo, por vezes, quando falamos de casos de *ransomware* violentos e que minam todo o sistema, por exemplo, de uma PME), podendo levar à própria falência de uma empresa e à extinção de uma marca; tal pode ser o cenário devastador e as consequências catastróficas de um ciberataque de sucesso.

O ambiente de teletrabalho promoveu um certo descuido face às medidas de segurança, o que faz com que todos, mesmo os mais formados, estejam "menos alerta" para eventuais ameaças ou comportamentos suspeitos. Os níveis de maturidade de segurança variam de organização para organização, mas o fator humano é normalmente a maior fragilidade. As pessoas precisam de ser formadas para responderem a esta nova realidade e poderem novamente conviver com o mundo cibernauta, com tudo o que acarreta, de forma ponderada e responsável. Mais do que literacia digital, há a necessidade de haver literacia em cibersegurança.

É necessário prevenir e investir em modelos de segurança contínuos, conhecer bem as infraestruturas, e sobretudo, "stressar" os sistemas, procurando falhas e fragilidades, corrigindo-as de forma perseverante, de modo a "blindar" a organização contra quaisquer eventuais tentativas de ataques. Em simultâneo, e através de tecnologia, procedimentos, mas também através de testes de *stress*, deve testar-se vezes sem conta a nossa capacidade de recuperação a um incidente de segurança que possa implicar desastre global na organização. Conhecer a nossa capacidade de recuperação a um ciberataque é hoje fundamental para a gestão de qualquer empresa ou organização de modo a garantir a sua sobrevivência.

visionware

Challenging an Unsafe World

LEALDADE

DISCRIÇÃO

DEDICAÇÃO

A nossa missão é contribuir para o Sucesso dos nossos clientes, aumentando a sua cultura e maturidade em Segurança da Informação.

SERVIÇOS

- CYBERSECURITY
- CYBER DEFENSE OPERATIONS CENTER - SOC & CSIRT
- FORENSIC INVESTIGATIONS
- PRIVACY & LEGAL - GDPR | RGPC | WHISTLEBLOWING
- ETHICS & CORPORATE COMPLIANCE
- STRATEGIC INTELLIGENCE & RISK ANALYSIS
- PROFESSIONAL SERVICES
- TRAINING | VISIONWARE ACADEMY

SCAN ME

VISIONWARE.PT

visionwaresi

geral@visionware.pt

+351 225 323 740

PORTUGAL
Porto | Lisboa

CABO VERDE
Praia | Mindelo