



OPINIÃO

Zona cinzenta da segurança: o risco invisível da IA através do comportamento humano e da linguagem

Felipe Costa (*)

A inteligência artificial entrou nas organizações como promessa de eficiência, aceleração e ganho de produtividade, mas aos poucos passou a ocupar também um espaço mais sensível: o de interlocutora de decisões, análises e até de informações que, em outro contexto, jamais circulariam fora de ambientes controlados.

É nesse deslocamento silencioso que nasce um dos riscos mais subestimados da atualidade e existe uma diferença sutil, e perigosa, entre usar tecnologia e confiar demais nela.

A superfície de risco deixou de ser exclusivamente técnica e passou a ser comportamental, estrutural e, em muitos casos, invisível. A IA não precisa ser “invadida” no sentido tradicional. Ela pode ser manipulada por dentro, a partir da forma como interage com dados, instruções e contextos.

É nesse cenário que surgem vetores como prompt injection, onde instruções maliciosas são embutidas em entradas aparentemente legítimas para distorcer o comportamento do modelo. Em paralelo, a manipulação de agentes de IA amplia esse risco ao permitir que sistemas autônomos tomem decisões baseadas em contextos corrompidos ou induzidos, sem que o usuário perceba a origem da interferência. Não se trata mais de quebrar barreiras, mas de reprogramar respostas a partir da linguagem.

Ao mesmo tempo, cresce um vetor igualmente sensível: o vazamento de dados via chat-bots corporativos. Ferramentas integradas ao ambiente de trabalho, muitas vezes treinadas ou alimentadas com informações internas, passam a concentrar um volume significativo de dados estratégicos. Quando não há governança adequada, esses sistemas deixam de ser apenas assistentes e se tornam potenciais pontos de exposição, especialmente quando integrados a fluxos amplos, com pouca visibilidade sobre retenção, uso ou reprocessamento de informações.

O problema se intensifica quando se observa o comportamento humano dentro desse ecossistema. Funcionários, em busca de agilidade, eficiência ou

simplesmente praticidade, acabam alimentando IAs públicas com informações confidenciais sem plena consciência do impacto disso. Estratégias, dados de clientes, contratos e análises internas passam a circular em ambientes fora do perímetro corporativo, criando uma nova forma de vazamento que não depende de ataque externo, mas de uso cotidiano.

Segundo pesquisa do Gartner, de 2025, mais de 40% dos incidentes de segurança envolvendo inteligência artificial até 2027 estarão ligados ao uso inadequado de IA generativa dentro das organizações, especialmente pelo compartilhamento indevido de dados sensíveis em ferramentas não governadas. Em paralelo, a Tenable aponta que 70% das cargas de trabalho de IA em nuvem já apresentam vulnerabilidades não corrigidas, ampliando a superfície de exploração em um ambiente que cresce mais rápido do que sua maturidade de segurança.

Zona cinzenta

O que esses dados revelam não é apenas um problema tecnológico, mas uma lacuna de governança. A ausência de diretrizes claras transforma a IA em uma zona cinzenta, onde produtividade e risco coexistem sem fronteiras definidas. É justamente nessa zona que os ataques mais sofisticados encontram espaço, não porque quebram sistemas, mas porque exploram sua abertura conceitual.

Diante disso, a resposta não pode ser apenas reativa. Falar de segurança em IA hoje significa falar de governança desde a origem, classificação de dados como princípio estrutural e adoção de modelos de Zero Trust aplicados não apenas à rede, mas também às interações com inteligência artificial. Porque, se cada prompt pode carregar contexto sensível, então cada interação precisa ser tratada como um potencial ponto de exposição.

No fim, a pergunta mais relevante não é se a IA pode ser manipulada. Ela já pode. A questão real é o quanto as organizações estão preparadas para operar em um ambiente onde a linguagem se tornou uma superfície de ataque, e onde proteger dados significa, cada vez mais, proteger também a forma como pensamos ao interagir com máquinas.

(*) Engineering Sales Specialist da Adistec Brasil.



News@TI

Poli Digital recebe certificação técnica da Meta para operar soluções oficiais do WhatsApp Business

@A Poli Digital recebeu a certificação WhatsApp for Business Technical Certified Company. “Essa certificação reflete uma evolução natural da forma como as empresas vêm estruturando o uso do WhatsApp. Hoje, não se trata apenas de estar presente no canal, mas de operar com consistência, segurança e capacidade de escala, dentro dos padrões exigidos pela plataforma”, destaca Alberto Filho, CEO da Poli Digital. A certificação ocorre em um momento de consolidação dos aplicativos de mensagens como infraestrutura de relacionamento entre marcas e consumidores (https://poli.digital/).

Mais um alerta sobre a bolha da inteligência artificial

Há mais de um ano, analistas vêm alertando que a bolha da inteligência artificial, a supervalorização das empresas e tecnologias ligadas à IA não poderá durar muito tempo.

Vivaldo José Breternitz (*)

Apesar disso, ela segue inflada, a ponto de alguns indicadores relativos à economia dos Estados Unidos mostrarem números piores do que os das vésperas da querbra da Bolsa de Nova Iorque, que ocorreu em outubro de 1929 e marcou o início da Grande Depressão, a mais devastadora crise econômica da história moderna

Segundo Russ Mould, colunista de economia do jornal britânico *The Daily Telegraph*, a supervalorização das ações americanas já ultrapassou o nível que levou o mercado ao crash de 1929.

Ele observa que os papéis que compõem o índice S&P 500 estão sendo negociados a cerca de 42 vezes a média dos lucros da última década, índice conhecido como Shiller CAPE (Cyclically Adjusted Price-to-Earnings Ratio), em homenagem ao professor e economista ganhador do Nobel Robert Shiller.

Em outras palavras, investidores estão pagando US\$ 42 por cada US\$ 1 de lucro médio anual gerado pelo índice nos últimos dez anos.

É, nas palavras de Mould, o equivalente financeiro à maré recuando antes de um tsunami. Não é possível prever exatamente quando a onda virá, nem seu tamanho, mas um Shiller CAPE tão elevado indica perigo. Para efeito de comparação, a média histórica é de 17,3, segundo o site *Investing.com*. Na chamada “Black Tuesday”, dia em que se iniciou o crash de 1929, o índice estava em 32,5, quase nove pontos abaixo do nível atual.



A justificativa para preços tão altos repousa quase inteiramente na crença do sistema financeiro americano de que a IA inaugurará uma revolução permanente em produtividade e lucros, embora na prática ela ainda não tenha alterado para melhor a produtividade da maioria dos locais onde vem sendo usada.

Há algumas semelhanças entre o cenário atual e aqueles vividos quando da difusão da internet nos anos 1990 e da eletrificação nos anos 1920. Em ambos os casos, as tecnologias foram incorporadas ao cotidiano, mas não antes do entusiasmo desmedido gerar desastres financeiros.

Uma situação como a atual só pode ser resolvida de duas formas: ou os lucros gerados pela IA alcançam as projeções

Empresários invisíveis na internet podem perder espaço em um mercado guiado por buscas online

Pesquisar nomes, organizações e trajetórias profissionais tornou-se uma prática recorrente entre consumidores, investidores e potenciais parceiros comerciais. Em muitos casos, a impressão inicial é formada em poucos minutos, a partir de resultados de busca, notícias, perfis institucionais e conteúdos publicados em plataformas digitais. Quando essas informações são escassas, desatualizadas ou inexistentes, abre-se espaço para dúvidas, leituras incompletas e perda de competitividade.

Buscadores e redes sociais passaram a concentrar e hierarquizar conteúdos, funcionando como ponto de partida para a formação de impressões sobre pessoas e organizações. Nesse contexto, a consistência e a presença de dados públicos são determinantes para reduzir incertezas e sustentar a credibilidade. Estar ausente ou pouco representado nesse ambiente significa abrir mão de influenciar a própria narrativa e permitir que a percepção seja construída por lacunas de informação.

Para mitigar esse impacto, a construção de presença digital deixou de ser uma ação pontual e passou a exigir posicionamento contínuo. Manter canais institucionais atualizados, compartilhar conhecimento por meio de artigos e entrevistas, fortalecer a atuação em redes profissionais e participar de debates relevantes são iniciativas que ampliam a visibilidade e ajudam a construir autoridade junto a públicos de interesse.



A reputação digital é resultado de um processo constante de fortalecimento da imagem institucional. Quanto maior a qualidade e a frequência dos dados disponibilizados publicamente, maiores são as chances de empresas e lideranças serem reconhecidas por sua experiência, seus diferenciais e suas contribuições para o mercado.

Esse processo é ampliado pela evolução da inteligência artificial. Diferentemente dos buscadores tradicionais, que organizam links e referências, ferramentas de IA sintetizam informações disponíveis na internet para gerar respostas diretas. Com isso, a forma como empresas e profissionais estão representados em fontes abertas passa a influenciar diretamente

fantasiosas feitas por seus entusiastas, ou o mercado de ações sofrerá queda muito violenta, arrastando consigo a economia real.

Como a primeira alternativa parece cada vez menos provável, dentro de não muito tempo, talvez o mundo viva tempos semelhantes aos da Grande Depressão, que no Brasil impactou fortemente a cafeicultura, à época a base da economia do país, gerando desemprego generalizado, derrubando preços e exportações, abrindo caminho para a Revolução de 1930 e a ascensão de Getúlio Vargas, que redefiniu nossa história.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjntz@gmail.com.

HP apresenta inovações em impressão sustentável e fluxos inteligentes de produção na FuturePrint 2026

A HP está marcando presença na FuturePrint 2026, principal evento da América Latina voltado à comunicação visual, serigrafia e impressão digital têxtil, apresentando inovações em seu portfólio de impressão de grande formato com foco em produtividade,

sustentabilidade e automação. A edição deste ano acontece de 14 a 17 de julho, no novo e moderno Distrito Anhembi, em São Paulo. A empresa está comprometida em oferecer soluções que unam inovação tecnológica, responsabilidade ambiental e eficiência ope-

racional para contribuir com a transformação do ambiente de trabalho gráfico. A proposta é apoiar os PSPs (prestadores de serviços de impressão) na adaptação a um mercado cada vez mais exigente e conectado (http://www.hp.com).

 José Hamilton Mancuso (1936/2017) Responsável: Lilian Mancuso	Laurinda Machado Lobato (1941-2021)	José Leonil Lobato (1939-2026)
Editorias <i>Economia:</i> Nelson Tucci (nelson.tucci@netjen.com.br) <i>Mercado/Negócios/Tecnologia/Agronegócios/ Espaço empresarial:</i> Ricardo Souza (ricardosouza@netjen.com.br); <i>Livros:</i> Ralph Peter (ralphpeter@agenteliterarioralph.com.br) <i>Comercial:</i> comercial@netjen.com.br <i>Publicidade Legal:</i> lilian@netjen.com.br	<i>Webmaster/TI:</i> Fabio Nader; <i>Editoração Eletrônica:</i> Ricardo Souza. <i>Revisão:</i> Maria Cecília Camargo; <i>Serviço informativo:</i> Agências Brasil, Senado, Câmara, EBC, ANSA. Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.	Jornal Empresas & Negócios Ltda Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080 Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br) Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90 JUCESP, Nire 35218211731 (6/6/2003) Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.
Colaboradores: Ana Luisa Winckler, Carol Olival, Claudia Lazzarotto, Denise Debiasi, Fabiana Monteiro, Geraldo Nunes, Heródoto Barbeiro e Neiva Mendes	ISSN 2595-8410	