OPINIÃO

Vazamento de dados em conversas com IA levanta alerta de privacidade

Atilla Arruda (*)

Nos últimos meses, diversos incidentes expuseram publicamente conversas privadas de usuários com chatbots de inteligência artificial, acendendo um sinal de alerta sobre vazamento de dados e proteção da privacidade.

Diálogos confidenciais mantidos em plataformas de IA – que muitos julgavam ser privados – acabaram indexados no Google e outros buscadores, tornando-se acessíveis a qualquer pessoa online. Casos envolvendo serviços populares como ChatGPT, a assistente Meta AI e o chatbot Grok da xAI deixam claro os riscos na forma como essas ferramentas lidam com os dados dos usuários.

Incidentes recentes de conversas expostas por IA

No final de julho de 2025, usuários descobriram que milhares de conversas feitas no ChatGPT estavam aparecendo em resultados de busca do Google de forma inadvertida. Um novo recurso experimental da OpenAI chamado "Tornar esta conversa detectável" permitia que diálogos com o chatbot ficassem públicos e fossem encontrados via pesquisa web.

A intenção era ajudar pessoas a descobrir conversas úteis, mas, na prática, muitos ativaram essa opção sem entender as implicações, expondo conteúdos sensíveis. Diante da repercussão negativa, a OpenAI rapidamente removeu o recurso no dia 31 de julho de 2025.

Em outro caso, envolvendo a Meta, os diálogos dos usuários com a IA das plataformas da empresa - Facebook, Instagram e WhatsApp foram publicados online, sem aviso. No mesmo período, a startup xAI, de Elon Musk, viu seu chatbot Grok protagonizar outro vazamento em massa. Assim como nos casos anteriores, o problema estava na função de "compartilhar" conversas. Ao compartilhar um diálogo no Grok, a plataforma gerava um link público no site do próprio chatbot – que acabava indexado por motores de busca como Google, Bing e DuckDuckGo.

Investigações revelaram que mais de 370 mil conversas de usuários com o Grok já se encontravam listadas no Google. Muitos usuários ficaram surpresos ao descobrir que seus chats privados estavam públicos, pois não houve um alerta claro sobre essa possibilidade.

Governança de dados e prevenção de vazamentos

Os exemplos acima mostram a necessidade das empresas em fortalecer a governança de dados, especialmente no que tange ao uso das plataformas de IA.

Um estudo realizado pelos pesquisadores Carmen Bonifácio e Fábio Porto – do Instituto de Inteligência Artificial do LNCC, e Fernando Schapachnik, da Universidad de Buenos Aires, e publicado em maio deste ano, mostra a complexa relação entre a IA e a transformação do trabalho na América Latina. A pesquisa aponta que ao menos 39% disseram que o uso de IA generativa já faz parte da sua rotina diária de trabalho, e 61% relataram aprender a usar IA por conta própria, principalmente pela internet, sem apoio organizacional estruturado.

Ou seja: há um contingente expressivo de trabalhadores brasileiros que já incorporam IA generativa no dia a dia profissional, mas de forma autônoma e sem orientação oficial das empresas. Esse cenário aumenta os riscos de mau uso, exposição inadvertida de informações e ausência de governança, já que o aprendizado é autodidata e muitas vezes feito fora do horário de trabalho. Em última instância, o que ocorreu com ChatGPT, Meta AI e Grok — conversas privadas tornadas públicas por falta de controles claros — pode se repetir dentro das organizações se não houver políticas definidas.

No âmbito corporativo, esses incidentes reforçam porque muitas organizações têm sido cautelosas ao adotar IAs generativas. Empresas lidam com dados confidenciais de clientes e segredos comerciais que poderiam vazar caso funcionários utilizem ferramentas sem as devidas salvaguardas. Por isso, cresce o interesse em soluções de IA empresariais com foco em privacidade e controle. A Microsoft, por exemplo, integrou assistentes de IA em suas plataformas, assegurando a governança e a segurança dos dados.

As solicitações e respostas geradas pelo Copilot permanecem dentro do ambiente protegido do Microsoft 365 – ou seja, não são expostas externamente – e são criptografadas durante o armazenamento. Além disso, os administradores da organização têm como auditar e definir políticas de retenção dessas interações através de ferramentas de compliance.

Diante desse cenário, fica claro que a governança de dados precisa estar no centro da estratégia corporativa de adoção de IA. Não basta implementar ferramentas sofisticadas: é essencial estabelecer políticas claras de uso, treinar colaboradores, definir limites de acesso e monitorar continuamente as interações com os modelos. Ao adotar plataformas empresariais que garantem confidencialidade e oferecer capacitação estruturada aos times, as empresas conseguem equilibrar inovação e segurança, evitando que o entusiasmo pelo uso da IA se transforme em risco de vazamento ou perda de confiança.

(*) Diretor Comercial da Solo Network.

OpenAI e Amazon assinam contrato de US$ 38 bilhões

A OpenAI firmou um acordo no valor de US$ 38 bilhões com a Amazon Web Services (AWS) para que esta processe seus produtos de inteligência artificial, como o ChatGPT e Sora.

SweetBunFactory_CANVA

Vivaldo José Breternitz (*)

O acordo garante à OpenAI acesso imediato a centenas de milhares de processadores gráficos da Nvidia, instalados em computadores da AWS e essenciais para treinar e executar seus modelos de IA.

A AWS começará a fornecer os serviços imediatamente, com toda a capacidade contratada disponível até o fim de 2026 e possibilidade de expansão em 2027 – o acordo tem validade de sete anos. Para atender a OpenAI, a Amazon pretende instalar chips de última geração, como os aceleradores Nvidia GB200 e GB300, em clusters de dados dedicados à geração de vídeos por IA, respostas do ChatGPT e treinamento de novos modelos.

A crescente demanda por modelos generativos de IA exige uma infraestrutura computacional robusta. Com a escassez global de chips nos últimos anos, encontrar fontes confiáveis tem sido um desafio. A OpenAI, inclusive, estaria desenvolvendo seu próprio hardware de GPU para aliviar essa pressão.

Sam Altman, CEO da OpenAI, revelou planos ambiciosos: investir US$ 1,4 trilhão para desenvolver 30 gigawatts de capacidade computacional, o suficiente para abastecer com energia elétrica cerca de 25 milhões de residências nos EUA. Ele também mencionou a meta de adicionar 1 gigawatt por semana, o que equivale à produção de uma usina nuclear típica. Cada gigawatt, segundo a Reuters, custa mais de US$ 40 bilhões.

As necessidades da OpenAI superam a capacidade da Microsoft, até então praticamente seu único provedor de serviços - ainda assim, esta continua essencial: as empresas assinaram contrato no valor US$ 250 bilhões para serviços de processamento.

A OpenAI também já havia firmado acordos com o Google em junho, e com a Oracle em setembro, para garantir infraestrutura adicional. O contrato com a Oracle prevê US$ 300 bilhões em poder computacional por cinco anos.

Apesar do entusiasmo dos investidores, o cenário da IA não é totalmente promissor. A receita anualizada da OpenAI deve atingir US$ 20 bilhões até o fim do ano, mas seus prejuízos também estão crescendo. Avaliações inflacionadas, investimentos circulares e compromissos bilionários levantam dúvidas sobre a sustentabilidade do setor - há quem diga que IA é uma bolha prestes a estourar.

Enquanto isso, a OpenAI estaria preparando uma oferta pública inicial de ações (IPO) no valor de até US$ 1 trilhão. Se esse valor faz sentido para uma companhia que consome recursos mais rápidamente do que os gera, é uma questão que ainda divide analistas e investidores.

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

O novo poder corporativo da era da IA está nas mentes, não nos modelos

A corrida global pela inteligência artificial não é apenas sobre quem constrói os modelos mais poderosos, e sim, sobre quem consegue manter as mentes que os constroem. A disputa por talentos de IA atingiu um novo patamar, e os dados mostram que essa guerra já move bilhões.

No Brasil, a participação das transações de fusões e aquisições envolvendo inteligência artificial quase quintuplicou em 2024, passando de 5% das operações totais em 2023 para 23% no ano passado, segundo levantamento do escritório BZCP, que analisou 70 transações com valores entre R$ 50 milhões e R$ 500 milhões. O movimento marca o retorno do crescimento após o índice estabilizar em 13% entre 2021 e 2022, um sinal claro de que a "compra de cérebros" virou parte central da estratégia de expansão corporativa.

A tendência é impulsionada por um ecossistema em franca transformação. Um estudo da Amazon Web Services (AWS) revela que 53% das startups brasileiras já utilizam IA em seus negócios, enquanto 31% estão desenvolvendo novos produtos baseados na tecnologia. O mesmo levantamento aponta que 78% acreditam que a inteligência artificial transformará seus setores nos próximos cinco anos.

Essa corrida ainda enfrenta um obstáculo crescente - a escassez de especialistas. Pesquisa global da Bain & Company, realizada com líderes corporativos de cinco países, mostra que 44% afirmam que a falta de expertise interna já atrasa a adoção da IA em suas empresas. No Brasil, o cenário não é diferente, 39% dos executivos de tecnologia relatam o mesmo desafio em 2025, um salto em relação aos 25% de 2024. A consequência é direta: salários em alta e rotatividade acentuada. A demanda por profissionais de IA cresce 21% ao ano, impulsionando remunerações e tornando a retenção de talentos uma vantagem competitiva por si só.

O episódio recente da Meta, que tentou atrair engenheiros das rivais como OpenAI e Anthropic mesmo após oferecer pacotes milionários, é emblemático. Ele mostra que a lealdade em tecnologia não se compra, se conquista. Bonificações escalonadas, golden handcuffs e planos de vesting prolongados ajudam na retenção de talentos, mas o verdadeiro motor é o propósito e o prestígio intelectual.

Mais do que cifras, o que retém profissionais de IA é a sensação de estar moldando o futuro. As empresas que entenderam isso criam culturas de aprendizado contínuo, liberdade criativa e impacto real - atributos que valem mais do que qualquer pacote de bônus. Nesse contexto, o diferencial competitivo deixou de ser o código-fonte e passou a ser quem escreve o código.

Em um mundo onde dados são commodities e modelos podem ser replicados, o capital intelectual se tornou o ativo mais escasso e estratégico do século XXI. E talvez a pergunta que definirá a próxima década não será quanto vale uma startup, mas quanto valem as pessoas capazes de criá-la.

(Fonte: *Por João Eliezer C. Guimarães, especialista em M&A e sócio-fundador da Camaya Partners)

News @TI

ricardosouza@netjen.com.br

CLM agora distribui Riverbed na América Latina

@CLM, distribuidor latino-americano de valor agregado com foco em segurança da informação, infraestrutura para datacenters, e Riverbed, líder em AIOps (Inteligência Artificial para Operações de TI) para observabilidade, firmaram acordo de distribuição para a América Latina. A aliança estratégica vai ao encontro de demandas urgentes de monitoramento e otimização contínua, especialmente em verticais como governo, empresas estatais, telecomunicações, provedores de serviços, instituições financeiras, grandes corporações e indústrias com operações distribuídas (www.CLM.tech).

20 startups de educação e futuro do trabalho concorrem a investimentos

@Com o objetivo de qualificar empreendedores de impacto para estarem aptos a acessar capital de forma mais estratégica, a Potencia Ventures e a Artemisia lançaram, em maio de 2025, o Potencia UP: Preparação para Investimentos de Impacto. Agora, na segunda fase, 20 negócios destaques foram selecionados para mentorias e acompanhamento individualizado com ênfase nos principais desafios apresentados durante a etapa de capacitação para, assim, concorrer a investimentos entre US$ 100 mil e 500 mil da Potencia Ventures (https://www.potenciaventures.net/).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

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.