OPINIÃO

A IA pode ver tudo, mas quem garante a privacidade dos dados públicos?

José Ricardo Maia Moraes (*)

A IA pode ver tudo, mas quem garante a privacidade dos dados públicos?

Essa pergunta persegue os especialistas do mercado desde que a inteligência artificial deixou de ser um experimento para se tornar uma necessidade operacional na cibersegurança do setor público. O volume de ataques, a sofisticação dos métodos e a velocidade com que as ameaças se propagam tornaram inviável depender apenas de controles tradicionais e análises manuais. Ainda assim, sempre devemos pensar que, introduzir IA nesse contexto é como trazer um holofote para uma sala escura, você enxerga mais, mas também expõe tudo.

Essa tensão está no centro das decisões estratégicas de qualquer órgão público que lida diariamente com dados sensíveis, sistemas críticos e serviços essenciais. Não é uma discussão teórica, é o dia a dia de quem precisa equilibrar proteção e privacidade.

IA como multiplicador de capacidade, não como substituto

Na prática, a principal contribuição da IA está na capacidade de observar o que antes era invisível. Já vimos modelos de aprendizado de máquina correlacionarem eventos que pareciam desconexos, identificarem padrões anômalos que passariam despercebidos por meses e anteciparem comportamentos maliciosos em ambientes complexos. Em vez de reagir apenas ao que conhecemos, esses sistemas aprendem o funcionamento normal das nossas infraestruturas e sinalizam desvios em tempo real. Isso reduz o tempo de detecção de semanas para horas, acelera nossa resposta e diminui a dependência de regras estáticas que, sabemos bem, envelhecem rápido demais para as ameaças atuais. No setor público, onde convivem tecnologias legadas, múltiplas redes e diferentes níveis de maturidade digital, essa capacidade de correlação não é apenas útil, é vital.

O ponto de inflexão, onde muitos projetos tropeçam, surge quando entendemos que a eficácia da IA depende do acesso a grandes volumes de dados. Logs, registros de acesso, comportamentos de usuários, tráfego de rede... tudo isso é essencial para treinar e operar modelos eficientes. Porém, sem os devidos cuidados, esse acesso pode transformar ferramentas de defesa em potenciais vetores de exposição. O risco, portanto, nunca esteve na tecnologia em si, mas na ausência de uma estratégia clara de proteção, governança e limitação de uso dos dados analisados. A IA aplicada à cibersegurança pública precisa operar com um princípio básico: ver padrões não significa ter direito a ver pessoas.

Criptografia e controle de acesso como pré-requisitos

É nesse contexto que a criptografia deixa de ser um componente técnico isolado e passa a ser um elemento estrutural da confiança digital. Dados usados por sistemas de IA devem estar protegidos em todas as fases, armazenamento, transmissão e processamento, com mecanismos que impeçam acesso não autorizado, mesmo em caso de comprometimento parcial do ambiente. Controles de acesso rigorosos, segregação de funções e políticas claras sobre quem pode interagir com dados e modelos não são opcionais. Em ambientes mais maduros, a IA analisa informações já protegidas, muitas vezes anonimizadas ou pseudonimizadas, reduzindo drasticamente o risco de exposição de dados pessoais. A lógica é simples, mas crucial: quanto mais inteligente o sistema, mais restrito deve ser o acesso aos dados que o alimentam.

Governança é o verdadeiro diferencial

A tecnologia, sozinha, nunca resolverá o dilema entre segurança e privacidade. O fator decisivo, e onde os projetos podem dar certo ou fracassar, é a governança. Isso inclui regras transparentes sobre coleta, uso e retenção de dados, mecanismos de auditoria que funcionem na prática, explicabilidade real dos modelos e supervisão humana constante.

No setor público, decisões automatizadas precisam ser rastreáveis e justificáveis. Não basta que um sistema indique uma ameaça; é preciso poder explicar por quê, com base em quais critérios e sob quais limites legais e institucionais. Os projetos bem-sucedidos são aqueles em que a IA nasce integrada a políticas de segurança da informação, proteção de dados e compliance, não como uma camada adicionada posteriormente para resolver problemas.

Um novo equilíbrio para a defesa digital

A inteligência artificial já é parte do presente da cibersegurança governamental. Ignorá-la significa aceitar níveis de risco incompatíveis com a relevância dos serviços públicos digitais. Ao mesmo tempo, adotá-la sem critérios claros compromete o ativo mais valioso do Estado: a confiança do cidadão.

O caminho viável, pelo que tenho visto nos casos que funcionam, passa por um equilíbrio pragmático. IA para ampliar visibilidade e resposta. Criptografia para proteger o que é sensível. Governança para garantir limites, transparência e responsabilidade.

A pergunta, portanto, não é mais se o setor público deve usar IA para se defender, mas como fazer isso sem cruzar linhas que não podem ser cruzadas. É uma linha tênue, mas é nela que trabalhamos todos os dias.

(*) CTO da Neotel.

Geração Z chegando à universidade sem conseguir ler adequadamente

A Geração Z é a formada por pessoas nascidas entre meados da década de 1990 e início dos anos 2010.

Vivaldo José Breternitz (*)

Corina_Ciocirlans_Images_CANVA

À medida que os últimos representantes da Geração Z passam pelo ensino médio e ingressam em universidades, professores de ensino superior relatam uma preocupante queda nas suas habilidades em termos de compreensão de textos. Diante desse cenário, muitas instituições têm recorrido a uma solução drástica: reduzir significativamente o nível de seus cursos.

A professora da Pepperdine University, Jessica Hooten Wilson, afirmou em entrevista à revista *Fortune* que o problema vai além incapacidade de pensar de forma crítica. "Não é sequer uma incapacidade de pensar criticamente. É uma incapacidade de entender frases", disse. A professora admite ter reduzido suas exigências acadêmicas diante da chegada de estudantes que mal conseguem lidar com textos básicos. Enquanto professor universitário, pensamos e agimos de forma similar.

O professor da Universidade de Notre Dame, Timothy O'Malley, também observa mudanças significativas. Ele lembra que, no passado, era comum atribuir entre 25 e 40 páginas de leitura por aula. Hoje, essa prática seria "impensável", pois segundo ele, muitos estudantes recorrem a resumos gerados por inteligência artificial e tem passado pela escola sem muito incentivo à leitura.

Especialistas apontam que a responsabilidade não é apenas dos jovens. O sistema educacional enfrenta sérias falhas, agravadas pela pandemia de COVID-19, além de uma cultura cada vez mais voltada para vídeos e conteúdos audiovisuais em detrimento da leitura.

A crise da Geração Z reflete uma tendência mais ampla. Nos últimos 20 anos, o número de adultos que leem por lazer nos Estados Unidos caiu 40%. Além disso, levantamento do Programa Internacional de Avaliação de Competências de Adultos (PIAAC) revelou que 59 milhões de americanos estão no patamar mais baixo de nível de leitura, em uma escala de cinco níveis.

O cenário sugere que, sem reformas estruturais profundas no sistema educacional, a Geração Z dificilmente será a última a apresentar índices de alfabetização piores do que os de seus antecessores, nos Estados Unidos e no Brasil.

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

A importância da previsibilidade de custos em cloud

A nuvem deixou de ser apenas um elemento tecnológico para se consolidar como uma ferramenta de negócios. No início, as empresas investiram em cloud computing com o único propósito de armazenar dados, porém, visto sua capacidade de gerar insights valiosos, as organizações perceberam o potencial de crescimento estratégico e financeiro. De acordo com a pesquisa Panorama Cloud nas empresas brasileiras, realizada pela TOTVS em parceria com a H2R Insights & Trends, 77% das empresas usam a ferramenta com foco em segurança, escalabilidade e inovação.

Alemedia.id_CANVA

O diferencial não está somente na nuvem em si, mas nas aplicações desenvolvidas sobre essa infraestrutura, que permitem operar grandes volumes de dados e aplicar técnicas avançadas de análise. Ao utilizar o poder de processamento e escalabilidade da cloud computing, essas soluções conseguem tratar informações com agilidade, organizá-las e entregá-las aos gestores de forma personalizada, de acordo com os objetivos de cada área do negócio. Com essa flexibilidade, há o gerenciamento de todos os dados em multiplataformas, de fácil acesso por qualquer dispositivo conectado na internet. Por conta disso, a nuvem se tornou primordial para direcionar a gestão com foco em resultados, porque planejamentos feitos sem bases de dados robustos e detalhados não possuem embasamento para definir metas reais e desenvolver estratégias condizentes com a capacidade operacional.

Enquanto a tecnologia disponibiliza os insumos, os profissionais colocam em prática suas habilidades de interpretação e entendimento do mercado. Integrados aos sistemas empresariais, os dados passam a ser estruturados de forma a apresentar as informações com clareza e facilitar a análise, permitindo comparações com o histórico de performance e resultados. Dessa forma, as equipes identificam novas oportunidades de serviços e produtos, gargalos que dificultam o crescimento, necessidades dos clientes, ineficiência nos processos empresariais e ainda preveem riscos.

Diante desses insights, ficou claro que a nuvem corporativa se tornou o centro de decisões financeiras e operacionais. No entanto, muitas organizações ainda enfrentam um problema silencioso: a imprevisibilidade dos custos em clouds públicas. Visto que o investimento não se resume à infraestrutura, há taxas de saída, cobranças por I/O, custos de suporte e variações cambiais, tornando o orçamento volátil, principalmente com cloud internacional. Segundo estudo da International Data Corporation (IDC), as companhias que adotam nuvens corporativas locais reduzem em até 21% os custos totais de operação quando comparadas a ambientes de data centers tradicionais.

Dessa maneira, a distribuição de recursos com direcionamento preciso, de acordo com o processo operacional e devolutiva financeira de cada solução, dá à gestão de TI um controle de gastos inteligente. A partir deste cenário, é possível identificar no primeiro momento redução de custos, mas a longo prazo, com um planejamento financeiro, conciliado a relatórios de desempenho dos recursos tecnológicos, é possível proporcionar à liderança uma visão da produtividade das organizações, para auxiliar em planejamentos futuros.

Isso mostra que a previsibilidade não se limita ao faturamento mensal. Mas, é essencial ter suporte imediato para acontecimentos inesperados e que exigem maior atenção. Além disso, a nuvem cria uma proximidade técnica e consultiva, por trabalhar com equipes de especialistas locais, ter menor latência de resposta e operar conforme a LGPD. Esse formato ainda apresenta uma grande vantagem competitiva: os serviços ofertados foram desenvolvidos dentro do contexto atual do comportamento e necessidade do público, agregando conhecimento especializado aos serviços personalizados. O resultado é previsibilidade operacional, o complemento direto da previsibilidade de custos.

(Fonte: Paulo Lima é CEO da Skynova, empresa destaque em serviços de e-mail corporativo, cloud computing e segurança digital).

News @ TI

ricardosouza@netjen.com.br

Software.com.br anuncia abertura de operações na Argentina

@ A Software.com.br reafirma sua vocação internacional ao anunciar oficialmente a abertura de operações na Argentina, ampliando sua presença na América Latina. A capital Buenos Aires foi escolhida como base da operação pela proximidade estratégica com parceiros que já atuam em diversos países da região e por sua relevância como centro de inovação e negócios. A decisão posiciona a companhia no coração de um dos principais polos tecnológicos, assegurando atendimento de excelência e o mesmo padrão técnico já reconhecido no Brasil, México e Colômbia (www.software.com.ar).

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.