Opinião

IA nos seguros: Tecnologia está disponível, mas a revolução já começou?

Paulo Cesar Pissardo (*)

O mercado de seguros brasileiro tem apresentado números robustos. A CNseg projeta crescimento de cerca de 8% para 2026.

Contudo, esse dado não deixa clara uma contradição importante: a Inteligência Artificial (IA) já está amplamente presente nas operações, mas ainda distante de se tornar um verdadeiro diferencial competitivo. Cerca de 80% das seguradoras no país já implementaram algum tipo de IA, um número próximo aos 84% observados nos EUA. Ainda assim, os impactos por aqui seguem majoritariamente incrementais, com ganhos de até 1% de receita, enquanto o mercado americano já começa a registrar efeitos substanciais em escala.

A pergunta que emerge é direta: se a tecnologia está disponível, o que impede que agentes de IA transformem, de fato, a jornada das seguradoras e de seus clientes?

Parte da resposta está na própria natureza do mercado. O seguro ainda é um produto reativo, ou seja, ele não nasce do desejo, porém da dor. O consumidor médio não acorda disposto a contratar proteção; ele o faz após uma perda, um susto ou um evento extremo. Esse comportamento limita tanto a demanda quanto o incentivo à inovação mais agressiva. Em um país onde o endividamento das famílias pressiona decisões financeiras, o seguro frequentemente perde prioridade, o que impacta diretamente o apetite das seguradoras para aportes mais robustos em tecnologias como agentes autônomos. Ainda assim, os investimentos projetados pelo setor chegam a R$ 2,6 bilhões até 2026.

Ao mesmo tempo, há um descompasso estrutural onde a IA está sendo aplicada e onde ela poderia gerar mais valor. No Brasil, o uso ainda se concentra em back-office (análise de documentos, atendimento e operações de sinistro), enquanto aplicações mais estratégicas, como subscrição inteligente, prevenção de risco e fraudes, e orquestração de jornadas completas com agentes, permanecem subexploradas. O resultado é um ciclo de baixo impacto: sem casos de uso transformacionais, os investimentos permanecem conservadores; sem investimento, não há escala nem ruptura. Sobretudo em um setor que não conta com uma cultura de experimentação madura, no qual as seguradoras sabem que precisam da tecnologia, mas ainda estão descobrindo como fazê-la gerar valor real - e não apenas piloto após piloto sem escala.

Outro entrave crítico está na experiência real do cliente, especialmente no momento mais sensível: o sinistro. Mesmo seguradoras com alto nível de serviço ainda operam com processos fragmentados, dependentes de múltiplos sistemas e etapas manuais. O cliente, já fragilizado por uma perda, precisa repetir informações, aguardar validações e lidar com fluxos pouco integrados. É justamente aqui que agentes de IA poderiam atuar como orquestradores, automatizando a abertura de sinistros, interpretando documentos como boletins de ocorrência, validando evidências por vídeo e acelerando decisões.

Há também uma barreira menos visível, mas igualmente relevante: governança. O avanço dos agentes de IA exige mais do que tecnologia, demandando controle, padronização e estratégia. Sem isso, o risco é reproduzir um fenômeno já conhecido nas empresas: o "shadow IT". Assim como planilhas desestruturadas dominaram áreas de negócio no passado, agentes podem se proliferar sem coordenação, criando riscos operacionais, de segurança e de conformidade. Muitas seguradoras, conscientes desse desafio, avançam com cautela, algo que, por outro lado, retarda a inovação. Não por acaso, 69% das seguradoras enxergam a integração com sistemas legados como um relevante empecilho.

A questão da fraude adiciona outra camada de complexidade. Diferentemente de setores como o financeiro, onde transações podem ser rapidamente revertidas ou bloqueadas, o pagamento de sinistros envolve valores elevados e riscos permanentes. A autonomia dos agentes, desta forma, ainda é limitada pela necessidade de validação humana, especialmente em mercados como o brasileiro, onde a confiança institucional e os mecanismos antifraude ainda estão em evolução. Isso reforça um modelo híbrido, no qual a IA apoia, mas dificilmente decide sozinha, ao menos no curto prazo.

De forma inversa, o contexto externo reforça a urgência dessa transformação. Eventos climáticos extremos, como os registrados recentemente no Brasil, aumentam a percepção de risco e podem impulsionar a demanda por seguros. Ainda assim, a lacuna de proteção permanece enorme: apenas cerca de 17% das residências brasileiras possuem seguro, e menos de 20% das perdas econômicas causadas por desastres são efetivamente cobertas na América Latina. Isso revela um mercado com enorme potencial e, ao mesmo tempo, um desafio estrutural de acesso, educação e distribuição.

O que falta para os agentes de IA "pegarem" no setor de seguros não é tecnologia, mas convergência. Falamos da união entre dados de qualidade, sistemas integrados, governança sólida e, principalmente, modelos de negócio que coloquem o cliente no centro da jornada. Enquanto isso não acontece, os agentes continuarão sendo ferramentas promissoras em busca de um problema maior para resolver. O verdadeiro ponto de virada virá quando eles deixarem de ser assistentes isolados e passarem a operar como arquitetos invisíveis da experiência, reduzindo fricção, antecipando riscos e, talvez, tornando o seguro menos reativo e mais presente no dia a dia das pessoas.

(*) Head of Insurance Brazil da GFT Technologies.

Talibã proíbe smartphones

O Afeganistão segue marchando para o atraso: o Talibã proibiu o uso de smartphones por funcionários públicos e por seus próprios membros. Acredita-se que a qualquer momento essa proibição possa atingir o restante da população.

Vivaldo José Breternitz (*)

Zurijeta_CANVA

A notícia foi veiculada pelo jornal britânico *The Guardian*, que faz menção a um vídeo que vem circulando pela internet, onde um oficial talibã aparece comunicando a proibição, curiosamente usando um smartphone, enquanto outro indivíduo destrói aparelhos. O documento diz que "se alguém usar um celular, ele será quebrado e punições legais e da sharia serão aplicadas ao infrator". A sharia é a lei islâmica, e exceções só poderiam ser concedidas pelo líder supremo do país, Hibatullah Akhundzada.

Notícias provenientes do Afeganistão dão conta que a aplicação da medida ocorre de forma irregular: em algumas regiões, atinge apenas funcionários do governo; em outras, já se estende a mulheres, profissionais de saúde, professores, estudantes etc.

A decisão surge em meio a esforços crescentes do Talibã para isolar o país. Em setembro, autoridades ordenaram um bloqueio da internet por dois dias, justificando-o como forma de "prevenir a imoralidade". O apagão paralisou o comércio, afetou serviços de emergência e até a aviação.

Entre os fatores que podem ter impulsionado a proibição está a onda de protestos em Herat, a terceira maior cidade afegã, após prisões de mulheres e meninas por "uso inadequado do hijab", o véu cujo uso é obrigatório. Vídeos das manifestações mostraram o Talibã disparando contra a multidão, matando pelo menos duas pessoas.

Ainda antes dos protestos, porém, já havia restrições ao uso de celulares, motivadas por temores de vazamentos de informações e pela percepção de que os aparelhos reduziriam a produtividade dos funcionários públicos: em Herat, servidores relataram que seus telefones foram confiscados e destruídos.

Problemas como perda de tempo online e vazamento de informações podem acontecer em qualquer ambiente, público ou privado. A diferença está em como esses problemas são enfrentados e a escolhida pelo Taliban certamente não é a melhor para o país.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e membro da Congregação da Faculdade de Medicina de Jundiaí – vjnitz@gmail.com.

Sem cibersegurança não existe continuidade operacional

Para roubar uma carga no Brasil hoje, nem sempre é preciso parar o caminhão.

Criminosos passaram a explorar vulnerabilidades nos sistemas de rastreamento e gestão logística para acessar dados de rotas, manipular informações e viabilizar desvios sem nenhum confronto físico. É a convergência entre crime cibernético e crime físico, e ela está documentada nos dados que coletamos na INGENI, nossa divisão de inteligência da Redbelt Security.

Nos últimos três meses, o setor logístico brasileiro concentrou mais de 1.800 alertas de alta e crítica severidade relacionados a ransomware, vulnerabilidades exploráveis e movimentações de grupos criminosos. Quando se ampliam todos os níveis de criticidade, são mais de 58 mil alertas em 12 meses. Num setor que movimentou R$ 366 bilhões em 2024, algo em torno de 3,1% do PIB, e cujos portos sustentam 95% do comércio exterior do país, cada alerta tem endereço certo.

O setor logístico figura hoje entre os mais atacados globalmente. O ransomware somou 283 incidentes confirmados em 2025, segundo dados da Cyble. No Brasil, os ataques ao transporte de cargas dobraram. E o que os dados mostram é que os impactos já vão além da indisponibilidade de sistemas: o alvo é a informação que movimenta a operação.

BlackJack3D_CANVA

A superfície de ataque cresceu junto com a digitalização. Hoje, as operações logísticas dependem de um ecossistema que combina TI, tecnologia operacional e dispositivos conectados, como sensores, câmeras e plataformas telemáticas. Essa integração é o que garante rastreabilidade e eficiência em tempo real. É também o que amplia a exposição. Senhas padrão, sistemas desatualizados, ausência de segmentação entre redes... Vulnerabilidades conhecidas que continuam abertas porque corrigir exige parar, e parar tem custo.

Os portos concentram esse risco de forma especialmente visível. Funcionam como pontos de interconexão entre sistemas públicos, privados e internacionais, com alto volume de operações simultâneas. Quando um incidente acontece ali, os efeitos não ficam contidos no perímetro da autoridade portuária.

Uma parte relevante das vulnerabilidades, aliás, não nasce da tecnologia. Nasce das relações de confiança: fornecedores, operadores terceirizados, integrações com parceiros, usuários com credenciais mal gerenciadas. O perímetro de segurança no setor logístico é tão técnico quanto relacional.

A dificuldade estrutural é conhecida por quem opera no setor. A segurança não pode desacelerar a operação. Frotas não têm janela de manutenção. Centros de distribuição não fecham para atualização. Sistemas legados convivem com plataformas modernas porque substituí-los de uma vez é inviável. Nesse ambiente, maturidade em cibersegurança se mede pela capacidade de sustentar a operação mesmo sob pressão de um incidente.

Governança sólida, planos de resposta eficientes (e testados) e gestão de identidade para terceiros ainda são gargalos em muitas operações logísticas brasileiras. A consciência sobre o tema cresceu, mas a estrutura para lidar com ele ainda está sendo construída.

(Fonte: Eduardo Lopes é CEO da Redbelt Security).

News @ TI

ricardosouza@netjen.com.br

TD SYNNEX selecionada como parceira de distribuição global da HPE

@A TD SYNNEX foi selecionada pela HPE como uma de suas parceiras de distribuição global. A escolha apoia a transição da HPE para um modelo de distribuição mundial mais unificado, com foco em simplificar a forma pela qual os parceiros interagem com seu portfólio, o que permite uma execução mais consistente em todas as regiões e mantém o apoio a distribuidores regionais e especializados com atuação consolidada. À medida que a HPE continua a desenvolver sua abordagem de distribuição global, a TD SYNNEX apoiará a ativação do modelo em todas as regiões. (www.tdsynnex.com/na/us/hpe/).

Automação por IA provoca aumento nas fraudes e nos ataques cibernéticos

@NETSCOUT informa que a atividade de bots na internet atingiu um novo patamar. Segundo o relatório "Bad Bot 2025", do Thales Group, o tráfego automatizado já representa 51% de toda a atividade online global, superando pela primeira vez a atividade humana na web. Essa mudança marca uma transformação significativa no cenário digital e acende um alerta importante: aproximadamente 40% desses bots são maliciosos. O rápido avanço da automação digital está diretamente ligado aos progressos em inteligência artificial e outras tecnologias capazes de imitar o comportamento humano com alto grau de sofisticação (www.NETSCOUT.com).

Empresas & Negócios

José Hamilton Mancuso (1936/2017) | **Laurinda Machado Lobato (1941-2021)** | **José Leonil Lobato (1939-2026)**

Responsável: **Lilian Mancuso**

Editorias
Economia: Nelson Tucci (nelson.tucci@netjen.com.br)
Mercado/Negócios/Tecnologia/Agronegócios/
Espaço empresarial: 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: Ana Luisa Winckler, Carol Olival, Claudia Lazzarotto, Denise Debiasi, Fabiana Monteiro, Geraldo Nunes, Heródoto Barbeiro e Neiva Mendes

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.