



OPINIÃO

Fintechs na América Latina: a sustentabilidade na era pós-disrupção

O mercado de fintechs na América Latina entrou em uma nova fase.

Depois de anos marcados pela corrida para desafiar os bancos tradicionais e ampliar o acesso aos serviços financeiros, o setor agora enfrenta um teste mais complexo: provar que consegue crescer de forma sustentável.

O fim do ciclo de capital abundante, que impulsionou o ecossistema até 2021, mudou as prioridades dos investidores. Em vez de premiar apenas o crescimento acelerado da base de clientes, o mercado passou a exigir rentabilidade, eficiência operacional e modelos de negócio sustentáveis. Não por acaso, o mercado passou a falar nas chamadas "Séries P", em referência à lucratividade (*profitability*) como o novo diferencial competitivo das startups. Esse movimento também se refletiu na América Latina, onde o volume de capital permaneceu abaixo dos picos de 2021, mas passou a se concentrar em empresas com fundamentos financeiros mais sólidos e capacidade comprovada de geração de caixa.

Essa mudança também transformou a relação entre fintechs e consumidores. Em um estudo desenvolvido pela LatAm Intersect, identificamos um movimento que chamamos de Trust as a Service (TaaS): a confiança deixa de ser consequência da experiência do cliente e passa a ser um diferencial competitivo. O usuário latino-americano já não procura apenas uma conta digital ou um cartão. Ele espera que a instituição atue como um copiloto financeiro, oferecendo orientação personalizada com apoio de inteligência artificial.

Ao mesmo tempo, existe um limite claro para essa transformação. Embora 62% dos consumidores aceitem utilizar assistentes financeiros baseados em IA, 85% ainda preferem recorrer a uma pessoa em situações críticas, como fraudes ou disputas. A tecnologia amplia a eficiência, mas a confiança continua sendo construída por transparência, segurança e atendimento humano quando realmente importa.

Esse desafio se torna ainda maior diante do crescimento dos golpes digitais. A América Latina registra índices de ataques de phishing com inteligência artificial que ocorrem 40% mais do que a média global, tornando a segurança cibernética parte essencial da proposta de valor das instituições

Roger Darashah (*)
financeiras. Não basta oferecer inovação; é preciso comunicar com clareza como ela protege o cliente.

A própria inovação também mudou de significado. Hoje, inovar significa resolver problemas concretos da vida financeira das pessoas. O avanço das stablecoins ilustra bem esse movimento. Criadas inicialmente dentro do universo cripto, elas passaram a desempenhar um papel prático em economias marcadas por inflação elevada e restrições cambiais, facilitando remessas internacionais e preservação de valor. Na Argentina, por exemplo, já representam mais de 60% das transações com criptomoedas. A adoção não foi impulsionada pelo marketing, mas pela utilidade.

Essa lógica aparece em diferentes mercados latino-americanos. No México, cresce a demanda por recomendações financeiras personalizadas e por soluções voltadas ao mercado B2B. No Brasil, onde o consumidor mantém relacionamento com diversos bancos ao mesmo tempo, aumenta a expectativa por orientação financeira proativa e experiências integradas. Já países como Chile, Peru e Colômbia revelam que o desafio da inclusão financeira deixou de ser apenas abrir contas: agora é oferecer produtos relevantes, ampliar o acesso a investimentos e construir relações duradouras de confiança.

Segundo o relatório Global Findex 2025, do Banco Mundial, 70% dos adultos da América Latina e do Caribe já possuem uma conta em uma instituição financeira ou serviço de dinheiro móvel, um avanço significativo em relação aos 54% registrados em 2017. Com o acesso ao sistema financeiro cada vez mais consolidado, o principal desafio da próxima década deixa de ser apenas incluir mais pessoas e passa a ser construir instituições capazes de permanecer relevantes, rentáveis e confiáveis em um mercado cada vez mais digital.

A era da disrupção foi marcada pela competição para conquistar usuários. A era que começa agora será vencida por quem conseguir mantê-los. Em um mercado cada vez mais competitivo, produtos podem ser copiados rapidamente. Confiança, reputação e capacidade de resolver problemas reais, não. São esses ativos que definirão as fintechs que liderarão o próximo ciclo de crescimento da América Latina.

(*) Sócio e cofundador da LatAm Intersect.

News@TI

TeamViewer e ServiceNow firmam parceria
A TeamViewer, líder global em soluções para gestão de ambientes de trabalho digitais, e a ServiceNow, empresa de software que atua como centro de comando de Inteligência Artificial para reinvenção de negócios, anunciam uma parceria estratégica para integração das plataformas TeamViewer DEX e Conectividade Remota ao ambiente de IA da ServiceNow. O acordo plurianual entre as duas companhias que figuram no topo das mais inovadoras do setor de tecnologia contempla investimentos conjuntos para oferecer soluções de TI autônomas de ponta a ponta. Os recursos serão destinados a vendas e marketing para impulsionar uma abordagem global de go-to-market nas áreas de Gestão de Serviços de TI (ITSM), Gestão de Serviços de Campo (FSM) e Gestão de Atendimento ao Cliente (CSM). A parceria também prevê planos para aprofundar as integrações e fomentar a inovação, com o objetivo de expandir para novos casos de uso e mercados (www.teamviewer.com).

Agentes de IA estão atacando outros sistemas. De quem é a culpa?

Quando um agente de inteligência artificial invade os sistemas de uma empresa sem que nenhum humano tenha dado ordens nesse sentido, quem é o responsável? Ninguém sabe ao certo, mas isso começa a ser discutido.

Vivaldo José Breternitz (*)

A questão está longe de ser meramente teórica. Nas últimas semanas, agentes da OpenAI, da Anthropic e da Meta invadiram sistemas de outras organizações. O agente da OpenAI atacou o Hugging Face, uma das principais plataformas globais de colaboração em inteligência artificial e que reúne empresas e pesquisadores em torno de projetos da área.

Já a Anthropic, constatou que agentes seus invadiram sistemas de três outras empresas e a Meta disse que a invasão a sistemas de um parceiro ocorreu durante testes de segurança, em função de um erro humano.

Como destacou a revista *Wired*, se uma pessoa tivesse feito isso, responderia criminalmente. No entanto, a situação jurídica de um software é muito menos clara. Não existe uma norma estabelecida que obrigue a empresa criadora do agente a responder pelas ações do mesmo.

As normas jurídicas atuais não são claras em relação a casos como esses. As leis que tratam de crimes digitais pressupõem um invasor humano agindo intencionalmente. Normas de responsabilidade sobre um produto ou negligência poderiam alcançar o desenvolvedor, mas apenas se um tribunal decidir que um agente é um produto defeituoso ou um risco previsível. Nada disso está claro, e os agentes podem voltar a atacar.

Os órgãos reguladores dos Estados Unidos, onde estão sediadas as empresas criadoras desses agentes, já entraram em alerta. A Casa Branca está “avaliando me-



imaginima_CANVA

didadas de controle”, declarou o presidente Donald Trump ao ser questionado sobre as invasões. Na Europa, autoridades já discutem os incidentes e a tendência é que novas regras para sistemas autônomos sejam implementadas em breve.

Há consenso entre especialistas da área jurídica: as empresas devem ser responsabilizadas. Mas chegar a esse resultado, na prática é bem mais complexo. Isso exige definir se um agente é um produto, um serviço ou algo totalmente novo, além de determinar se a justificativa de que “a IA agiu por conta própria” pode ser aceita como defesa. Os tribunais, em todo o mundo, mal começaram a se debruçar sobre o tema.

Existe uma perspectiva mais objetiva para analisar o cenário. Alguém definiu uma meta, implantou um sistema para

alcançá-la e um ato ilícito ocorreu em seguida. Camadas de automação podem obscurecer essa cadeia de eventos, mas não apagam a decisão humana inicial. O desafio é traduzir essa intuição em uma responsabilidade civil executável pela Justiça.

Por enquanto, os incidentes se acumulam mais rápido do que as soluções. Fugas podem continuar a acontecer, os reguladores tentam estabelecer normas e as vítimas continuam sem uma resposta do sistema jurídico.

Os agentes de IA encontraram brechas nas defesas cibernéticas e também na legislação, e isso é perigoso para toda a sociedade.

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

Reconhecimento facial deixa de ser tendência e vira rotina no Brasil

Há poucos anos, utilizar o rosto para acessar um serviço parecia algo restrito à ficção científica. Hoje, desbloquear o celular, embarcar em aeroportos, acessar benefícios públicos ou entrar em um estádio utilizando apenas a biometria facial já faz parte da rotina de milhões de brasileiros. Mais do que uma inovação tecnológica, o reconhecimento facial tornou-se uma resposta à crescente demanda por praticidade, segurança e experiências mais fluidas.

Essa transformação acompanha um movimento global. Segundo estudo da consultoria Grand View Research, o mercado mundial de reconhecimento facial deverá superar US\$ 19 bilhões até 2030, impulsionado principalmente pelos setores de segurança, mobilidade, serviços financeiros e entretenimento. No Brasil, a tecnologia também avança rapidamente, impulsionada tanto pela iniciativa privada quanto pelo poder público.

Nos ambientes de grande circulação, como shows, festivais e eventos esportivos, essa evolução é ainda mais evidente. O reconhecimento facial deixou de ser apenas um mecanismo de controle de acesso para se tornar parte estratégica da operação. A identificação instantânea reduz filas, evita fraudes, impede o uso indevido de ingressos e melhora significativamente a experiência do público. O resultado é uma operação mais eficiente para os organizadores e mais confortável para quem participa do evento.

Não por acaso, a legislação brasileira passou a exigir sistemas de identificação biométrica em estádios com capacidade superior a 20 mil pessoas. A medida representa um novo paradigma para a gestão de grandes públicos, combinando tecnologia, segurança e agilidade em um único processo.

Esse movimento, porém, vai muito além do entretenimento. Recentemente, o Ministério de Portos e Aeroportos, em conjunto com a Agência Nacional de Aviação Civil (Anac), anunciou diretrizes para ampliar o uso da biometria na identificação de passageiros,



Divulgação

Tironi Paz Ortiz

“A identificação instantânea reduz filas, evita fraudes, impede o uso indevido de ingressos e melhora significativamente a experiência do público.

classificando a coleta desses dados como uma questão estratégica para a segurança nacional. A expectativa é acelerar o embarque, reduzir gargalos operacionais e elevar o nível de proteção dos aeroportos brasileiros.

Outro exemplo é o avanço da biometria na concessão de benefícios previdenciários e assistenciais. O Instituto Nacional do Seguro Social (INSS) ampliou a exigência do cadastro biométrico para aposentadorias, auxílios e Benefício de Prestação Continuada (BPC), buscando reduzir fraudes e garantir que os recursos cheguem aos beneficiários corretos. Ao mesmo tempo, a regulamentação prevê exceções para pessoas com mais de 80 anos e moradores de

regiões de difícil acesso, reconhecendo que a inclusão digital também precisa fazer parte dessa transformação.

Esse talvez seja um dos maiores desafios da expansão da biometria: garantir que a inovação seja acessível a todos. O avanço tecnológico precisa caminhar lado a lado com políticas de inclusão, interfaces intuitivas e alternativas para pessoas que possuem dificuldades de acesso ou menor familiaridade com ferramentas digitais. Afinal, a tecnologia deve simplificar a vida das pessoas, e não criar novas barreiras.

Outro ponto indispensável é a proteção dos dados. Informações biométricas são consideradas dados pessoais sensíveis pela Lei Geral de Proteção de Dados (LGPD) e exigem elevados padrões de governança, criptografia, controle de acesso, transparência e segurança cibernética. A confiança da população dependerá não apenas da eficiência da tecnologia, mas também da certeza de que seus dados estarão protegidos.

O futuro aponta para uma presença cada vez maior da identidade digital em diferentes setores da economia. Seja em eventos, aeroportos, instituições financeiras, serviços públicos ou no varejo, o reconhecimento facial tende a se consolidar como um padrão de autenticação. O desafio das empresas e dos órgãos públicos não será apenas implementar essa tecnologia, mas fazê-lo de forma ética, segura e transparente.

Mais do que substituir documentos ou acelerar acessos, o reconhecimento facial representa uma mudança na forma como as pessoas interagem com serviços. Quando utilizado com responsabilidade, ele deixa de ser apenas uma ferramenta tecnológica e passa a ser um elemento essencial para oferecer experiências mais simples, eficientes e seguras em um mundo cada vez mais conectado.

(Fonte: Tironi Paz Ortiz, CEO da Implify Tecnologia).

 José Hamilton Mancuso (1936/2017) Responsável: Lilian Mancuso	Laurinda Machado Lobato (1941-2021)	José Leonil Lobato (1939-2026)
Editórias <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	