OPINIÃO

Uso de biometria no setor financeiro: o paradoxo da inovação

STEFANO RIBEIRO FERRI

No último ano, o número de pessoas incluídas no Sistema Financeiro Nacional (SFN) ultrapassou a marca de 200 milhões, conforme dados do Banco Central. O avanço da bancarização reflete uma mudança profunda na forma como os brasileiros se relacionam com o dinheiro. A criação do Pix, a expansão dos bancos digitais e a consolidação do comércio eletrônico transformaram o acesso aos serviços financeiros. O resultado é uma inclusão inédita, com efeitos diretos sobre o desenvolvimento econômico, a redução de desigualdades e o acesso ao crédito.

Mas essa transformação, que amplia horizontes, também expõe milhões de pessoas a novos riscos. Conforme pesquisa da Febraban, 39% dos brasileiros já foram vítimas de algum tipo de golpe (ou tentativa) envolvendo suas contas bancárias. O setor financeiro vive um paradoxo: é referência mundial em inovação e, ao mesmo tempo, enfrenta o crescimento acelerado das fraudes virtuais. O desafio, portanto, é fazer com que inovação e segurança caminhem juntas.

Nesse contexto, a biometria passou a ocupar papel central nos processos de abertura de contas e no acesso a aplicativos bancários, funcionando como uma camada adicional de segurança. O uso de dados biométricos, como o reconhecimento facial, dificulta a ocorrência de fraudes. Ao mesmo tempo, trata-se de um dado pessoal extremamente sensível, pois, diferentemente das senhas, não pode ser alterado. Sua utilização exige padrões elevados de proteção, transparência e conformidade com as normas regulatórias.

O avanço tecnológico, no entanto, não foi acompanhado pelo letramento financeiro e pela conscientização da população. Milhões de pessoas não compreendem plenamente os riscos envolvidos nem a importância dos dados pessoais. Muitas vulnerabilidades não decorrem da tecnologia, em si, mas da desinformação.

Esse descompasso ficou evidente no episódio recente em que se formaram enormes filas na cidade de São Paulo de pessoas dispostas a fornecer a íris em troca de dinheiro. O caso chamou atenção não apenas pelo ineditismo, mas também por expor uma fragilidade social preocupante: a normalização da cessão de dados biométricos. Essas pessoas tinham plena ciência das possíveis consequências? Evidente que não. Trata-se de uma informação permanente e inalterável, cujo vazamento pode causar danos irreversíveis.

Não há dúvida de que a biometria, se utilizada de forma correta, torna-se uma das mais eficazes barreiras contra ações fraudulentas, protegendo o patrimônio e a identidade do consumidor. Entretanto, a segurança do sistema financeiro não depende apenas de aspectos técnicos, mas também de fatores culturais e educacionais.

É necessário um esforço conjunto. Instituições financeiras devem continuar investindo não apenas em tecnologias de proteção, mas também em comunicação clara e acessível com seus clientes. Ao Banco Central, cabe fortalecer as normas regulatórias e garantir que a tecnologia avance em consonância com a proteção do sistema financeiro. A sociedade civil, por sua vez, tem o papel de incentivar o debate público e a educação digital. Inovação financeira só se sustenta quando acompanhada de segurança, letramento e responsabilidade.

ESPECIALISTA EM DIREITO DO CONSUMIDOR E DA SAÚDE

STEFANO RIBEIRO FERRI/ARQUIVO PESSOAL/JC

Avanço da bancarização reflete uma mudança profunda na forma como os brasileiros se relacionam com o dinheiro

Governança algorítmica: como construir os alicerces de uma IA ética e confiável?

LEANDRO BONILLA

A Inteligência Artificial deixou de ser promessa e passou a ser parte essencial das estratégias de inovação em praticamente todos os setores da economia. Da criação de conteúdo à automação de processos corporativos, a IA hoje é protagonista nos negócios. Mas, à medida que os sistemas se tornam mais autônomos e decisivos, cresce também a necessidade de garantir que eles não cometam erros bruscos, principalmente, no âmbito ético e de governança.

Erros de IA podem assumir várias formas. Há os erros de programação, em que o modelo interpreta incorretamente uma instrução ou gera resultados inconsistentes; os erros de contexto, típicos de sistemas generativos que produzem respostas imprecisas ou inventadas; e os erros de viés, quando a IA reproduz padrões discriminatórios presentes nos dados de treinamento. Todos os tipos, embora diferentes em natureza, têm uma consequência comum: comprometem a confiabilidade da tecnologia.

Nos últimos meses, uma série de episódios reacendeu o alerta sobre os riscos do uso indiscriminado de modelos generativos. Um estudo conduzido pela Stanford School of Medicine mostrou que chatbots populares estão perpetuando ideias médicas racistas e equivocadas, chegando a formular equações falsas baseadas em raça. Sistemas amplamente utilizados podem, sem supervisão adequada, reforçar desigualdades históricas e disseminar informações incorretas.

Outro caso emblemático ocorreu no Brasil, quando uma imagem gerada por IA, mostrando um jovem negro segurando uma metralhadora observado por um policial branco, foi utilizada em uma sessão da Câmara dos Deputados. O episódio foi repudiado pelo Ministério da Igualdade Racial por perpetuar estigmas sobre a população negra periférica, um exemplo de como a falta de controle pode ter implicações sociais profundas.

Para superar esse desafio, a indústria caminha em direção a uma nova geração de soluções de IA: modelos híbridos, que unem o poder criativo da IA generativa à precisão e segurança da IA determinística. Essa combinação permite que os sistemas aprendam e se adaptem, mas dentro de limites claramente definidos por regras, padrões e validações automáticas.

É uma abordagem que transforma o desenvolvimento de software. Em vez de depender apenas de respostas probabilísticas, que podem variar e gerar inconsistências, as aplicações passam a se basear em estruturas lógicas auditáveis, garantindo rastreabilidade em cada decisão ou linha de código gerada. Assim, é possível reduzir drasticamente riscos de erros e evitar comportamentos indesejados, como o uso de linguagem ofensiva, a geração de informações incorretas ou a tomada de decisões sem transparência.

Além da segurança técnica, essa camada de controle reforça o compromisso ético das empresas que desenvolvem e utilizam IA. Em um cenário em que regulações como o AI Act europeu (regulamento da União Europeia sobre o uso da Inteligência Artificial na região) e legislações nacionais começam a exigir transparência e governança, soluções que nascem com princípios de aplicabilidade, auditabilidade e conformidade terão vantagem competitiva.

Outro aspecto decisivo é a gestão dos dados que alimentam esses modelos. Para que a IA seja realmente confiável, é essencial trabalhar com bases equilibradas e contextualizadas. Dados incompletos ou enviesados tendem a produzir erros sistêmicos, enquanto dados bem estruturados permitem que o sistema evolua com consistência e segurança.

O objetivo, portanto, não é apenas criar uma IA que funcione, mas uma IA que funcione bem e de forma responsável. Uma tecnologia que compreenda os limites de sua atuação, respeite diretrizes éticas e mantenha coerência técnica, independentemente da complexidade da aplicação ou do setor em que é usada.

O verdadeiro avanço da Inteligência Artificial não está em substituir o raciocínio humano, mas em potencializá-lo com segurança e confiabilidade. A próxima fronteira da inovação digital não será marcada apenas por sistemas mais rápidos ou criativos, mas por aqueles que não erram, nem na execução, nem na intenção.

REGIONAL MANAGER DA GENEXUS BY GLOBANT

GENEXUS BY GLOBANT/DIVULGAÇÃO/JC