

O Papel Estratégico da Inteligência Artificial na Prevenção de Fraudes Bancárias

A massiva migração para o *mobile banking*, que já responde por 75% das transações no Brasil, consolidou um novo campo de batalha para a segurança financeira, onde a conveniência para o cliente se tornou, paradoxalmente, a principal superfície de ataque para fraudadores. Essa transformação digital expôs o setor a uma nova classe de ameaças, com criminosos utilizando Inteligência Artificial (IA) para gerar *deepfakes* hiper-realistas, criar identidades sintéticas e lançar ataques de *phishing* que instrumentalizam a engenharia social com uma precisão algorítmica inédita. A magnitude do risco é sublinhada pelas perdas globais com fraudes, que ultrapassaram US\$ 485 bilhões em 2023. Diante dessa ofensiva, os métodos tradicionais de detecção, baseados em regras estáticas, provaram-se incapazes de competir com a dinâmica e a complexidade das ameaças, tornando-se não apenas inadequados, mas um passivo de risco inaceitável na arquitetura de segurança moderna.

Em resposta a essa escalada, a Inteligência Artificial e o *Machine Learning* (ML) emergiram como o imperativo estratégico do setor financeiro. O mecanismo central de defesa da IA reside na sua capacidade de processar volumes massivos de dados transacionais em tempo real para identificar padrões complexos, anomalias e comportamentos atípicos indetectáveis por sistemas convencionais. Para neutralizar o "fogo" dos criminosos – a própria IA Generativa usada para orquestrar ataques sofisticados – tornou-se essencial "combater fogo com fogo", utilizando a mesma tecnologia para fortalecer as defesas. Essa estratégia já é um padrão consolidado, com 90% das instituições financeiras utilizando soluções de IA para detectar atividades fraudulentas. Consequentemente, a IA deixou de ser uma vanguarda tecnológica para se tornar um componente indispensável não apenas para a defesa, mas para a própria sustentabilidade e resiliência operacional no ecossistema financeiro digital.

Essa transição para a IA não ocorre em um vácuo tecnológico, mas é impulsionada e moldada por um ecossistema robusto de governança regulatória e responsabilidade jurídica. O Banco Central do Brasil (BCB), em um movimento proativo, estabeleceu novas resoluções que tornam a segurança cibernética um processo contínuo e auditável, com exigências como o isolamento físico e lógico para sistemas críticos (Pix e STR) e a obrigatoriedade de testes de intrusão anuais. A exigência de um processo contínuo e auditável, por exemplo, torna os sistemas de IA, com sua capacidade de aprendizado e rastreabilidade em tempo real, a única contramedida viável para atender à nova régua regulatória. Paralelamente, a conformidade com a LGPD e a tramitação de marcos legais como o PL 2.338/23 impulsionam a necessidade de explicabilidade (*Explainable AI - XAI*) para mitigar os riscos do "problema da caixa-preta" dos algoritmos. Portanto, a efetiva implementação da IA na prevenção de fraudes é resultado da convergência estratégica

entre inovação tecnológica avançada, um arcabouço regulatório prescritivo e a crescente exigência de responsabilidade e transparência institucional.