Soluções baseadas em inteligência artificial, inteligência de dados e biometria facial serão essenciais para que empresas de diversos segmentos possam se prevenir contra ações criminosas

O ano de 2023 será bastante desafiador para as empresas de tecnologia especializadas no desenvolvimento de soluções de combate a fraudes. O cenário de riscos atual demandará o uso de soluções baseadas em inteligência artificial (IA), inteligência de dados (ID) e biometria facial, para que empresas de todos os segmentos possam se prevenir contra fraudes e crimes econômicos.

E por aqui, o problema parece ser maior do que nos outros países. Pesquisa da PwC, uma das maiores empresas de consultoria e auditoria do mundo, divulgada neste ano e intitulada "Protegendo o perímetro: o avanço da fraude externa" mostra que o índice de fraude, corrupção e crimes econômicos não registra aumento no mundo desde 2018. Pouco menos da metade das organizações globais (46%) relatou ter sofrido alguma forma de fraude ou outro crime econômico nos últimos 24 meses. Já no Brasil o percentual passou de 46% em 2020 para 62% em 2022.

Para a PwC "o desafio de gerenciar os riscos de novas fraudes é evitar cair na armadilha de ver apenas o que é conhecido". Vicente de Melo Pinheiro, diretor de engenharia da Stone Age ressalta que o mundo das fraudes é extremamente dinâmico e nem sempre é possível antecipar o tipo de golpe que será dado. Mas é possível identificá-lo rapidamente e tomar as medidas necessárias para não permitir que ele se propague.

"O importante é ser flexível e rápido. Nem sempre se trata de estar na frente e sim de ter uma resposta rápida. Precisamos estar preparados para fechar a porta o quanto antes", comenta o executivo, que destaca a inteligência artificial, a inteligência de dados e a biometria facial como as tecnologias que ganharão espaço no próximo ano.

"Eu destaco essas três por serem tecnologias desenvolvidas e aprimoradas nos últimos anos, mas que ainda não estão 100% difundidas. A biometria facial, por exemplo, ainda não é usada por todas as companhias. Mas é uma tecnologia essencial porque cada vez mais as empresas têm de se preocupar em oferecer segurança ao mesmo tempo que melhoram a experiência do cliente. Nesse ponto, a biometria contribui bastante para que o usuário não tenha de ficar preenchendo formulários ou respondendo perguntas", comenta.

Quanto à inteligência de dados, Pinheiro afirma, que ela nunca "morre" neste contexto porque os motores fazem o papel de avaliar score e documentos automaticamente, necessidades que não vão deixar de crescer em seu ponto de vista. "Mas também tem uma pegada de inteligência artificial entrando forte no mercado. As tecnologias já existentes tendem a evoluir com a implantação da IA, cujos algoritmos dão mais precisão às decisões. Por isso eu destaco essas três como as tecnologias antifraudes que devem evoluir bastante em 2023".

Saber escolher

O mercado de tecnologia oferece uma gama diversificada de soluções antifraude para empresas dos mais variados segmentos, resultando em uma dificuldade a mais para quem precisa implantar alguma ferramenta para proteger suas operações. Qual escolher, diante de tantas opções?

Pinheiro concorda que a escolha é difícil, até porque se trata de uma decisão bem estratégica. Mas há algumas perguntas importantes e que devem ser feitas na hora de a empresa compradora do serviço decidir o que implantar. São elas: Quais são os players que esse meu fornecedor já atende? Qual a relevância desse fornecedor que vai me dar essa solução antifraude ou algo do tipo dentro do mercado? Ele atende alguns players importantes?

"Se ele atende algumas empresas grandes já é um bom sinal. Tempo de mercado entra também. Temos de pensar um pouco se esse fornecedor tem escala, se é eficiente e flexível. Isso implica ter

a capacidade de implantar o sistema sem a necessidade de grandes mudanças estruturais, que demandaria tempo e altos custos", comenta complementando: "A Stone Age já atende nesse nível. Nos preocupamos bastante com a escala, com a eficiência e com a flexibilidade que cada contexto precisa".

Setores mais vulneráveis

Bancos e financeiras são, na atualidade, os maiores clientes dos serviços de proteção a fraudes e automação de processos. Isso porque eles precisam de segurança e agilidade para a concessão de empréstimos, abertura de contas digitais, entre outros. E com o início do Open Finance, sistema que permite o compartilhamento de dados – com a permissão do cliente – entre instituições financeiras, fica a expectativa de que novos tipos de fraudes possam surgir, o que manterá esse segmento no topo da demanda.

"Existe a ideia de que o Open Finance possa aumentar a vulnerabilidade a golpes, mas essas empresas também vão ter mais informações para tomarem decisões e elas vão precisar entender como tratar essas informações. Possíveis fraudes ou vulnerabilidades não são o maior foco, mas as empresas vão precisar se adequar muito rápido. Assim, se elas tiverem em mãos uma ferramenta que permita tomar decisões rápidas e assertivas e ao mesmo tempo aprenderem e evoluírem, elas vão conseguir evitar esses tipos de golpes ou novos tipos de fraudes que possam surgir".

Além do setor financeiro, despontam como novos possíveis clientes dos serviços de tecnologia de automação e controle de fraudes, companhias dos setores de Saúde, Educação e Locação de Veículos. "Identificamos um grande potencial nesses outros setores, que se digitalizaram bastante nos últimos anos. Estamos na fase de mapeamento desses segmentos".

No caso da saúde, por exemplo, uma dor latente é a prevenção de fraudes em pedidos de reembolso, que têm aumentado nos últimos anos. Já no ensino, um dos maiores desafios está relacionado à educação à distância, modelo que exige ferramentas mais eficazes de cadastro e controle dos alunos. Quando se trata de locação de veículos, o principal risco existente é a permissão de aluguel para criminosos que usam documentos falsos para pegar o veículo e nunca mais o devolvem.

"Nossas soluções podem ajudar empresas desses segmentos. E temos como diferencial a capacidade de modelar o produto à necessidade do cliente. Mapeamos as vulnerabilidades e mostramos qual tecnologia torna mais assertiva a decisão. Sem contar que não nos limitamos a sistema contra fraudes, trabalhamos com automação também e não vendemos apenas produtos de prateleira e sim um projeto para entregar o retorno que o cliente espera", conclui

Fonte: Compliance Comunicação, em 19.01.2023.