

Protegendo o presente, inovando para o futuro com IA responsável

Gerando melhores resultados em fraude e identidade



Sumário

Introdução

Protegendo o presente, inovando para o futuro

Página 3

Nossa abordagem

Escolhendo a IA pelos motivos certos

IA para ampliar o valor dos dados e aprimorar a detecção de fraudes

Página 4

Protegendo o presente

A busca contínua por melhores resultados para os clientes

Detecção de fraudes com IA: não apenas para scores de risco

Nosso compromisso com a IA responsável

Página 6

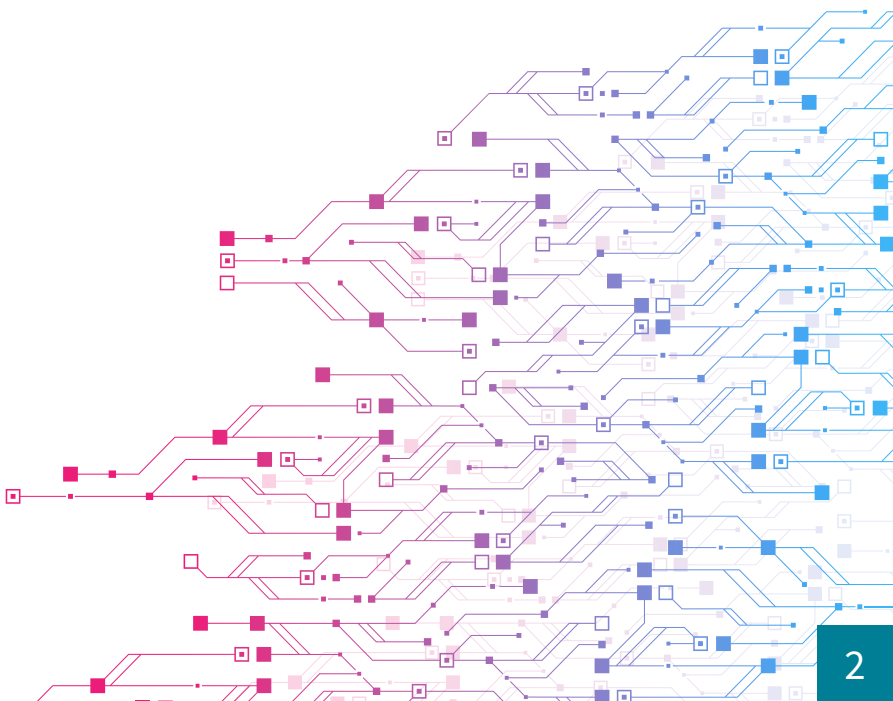
Inovando para o futuro

Ampliando suas possibilidades com a IA

Página 12

Considerações finais

Página 13



Protegendo o presente, inovando para o futuro com IA responsável

Gerando melhores resultados em fraude e identidade

A ascensão da inteligência artificial (IA), especialmente da IA generativa, gerou debates, preocupações e uma intensa movimentação em torno de controles e regulamentações em todo o mundo.

Há motivos legítimos para essa atenção, dada a percepção de “caixa-preta” da IA generativa e suas respostas ocasionalmente imprecisas. É também a primeira vez na história que uma metodologia sofisticada de IA foi democratizada a ponto de, literalmente, qualquer pessoa com um computador ou celular poder usá-la.

Essa democratização faz parecer simples mergulhar na IA para aplicações comerciais – mas não é. Usar a IA corretamente exige muito mais do que passar dados por um algoritmo.

Apesar da atenção que recebe atualmente, a IA existe há décadas, **e muito do que hoje chamamos de IA tem suas bases em métodos estatísticos já consolidados.** Na LexisNexis® Risk Solutions, usamos **análise de dados** há quase 25 anos. Nesse período, evoluímos nossas capacidades e metodologias de mineração de dados e de desenvolvimento de produtos orientados por IA, estabelecendo boas práticas pelo caminho. Nossa experiência ao longo desses projetos nos permitiu construir uma sólida base de capacidades em IA e desenvolver uma abordagem consistente para gerenciar os riscos e benefícios de sua aplicação nos negócios – incluindo o uso da IA para promover mais inclusão financeira e transparência.

Neste white paper sobre fraude e identidade, compartilhamos nossa jornada com a IA e mostramos como a LexisNexis® Risk Solutions utiliza a tecnologia de forma responsável para ajudar sua organização a enfrentar fraudes em constante evolução – seja prevenindo golpes de transferência autorizada no setor financeiro, prevenindo fraudes de tomada de conta (account takeover) no e-commerce ou protegendo pontos de fidelidade no setor de viagens. Tudo isso sem impactar a experiência das pessoas que dependem dos seus produtos e serviços.

Você verá como ajudamos a equilibrar a redução de atrito para clientes legítimos com o aumento das barreiras para agentes mal-intencionados.

A aplicação responsável da tecnologia, incluindo a IA, é parte fundamental de como ajudamos nossos clientes a alcançar melhores resultados, e continuará orientando nossa evolução nos próximos anos. Ao compartilhar nossa abordagem, buscamos demonstrar como podemos apoiar sua organização na solução de desafios complexos de fraude e identidade.

A LexisNexis® Risk Solutions trabalha com:

clientes em mais de **180**
países e diversos setores

9 dos 10 maiores
bancos do mundo

84% das empresas
da Fortune 500



Escolhendo a IA pelos motivos certos

A decisão de usar IA foi, desde o início, uma escolha ponderada. Embora sejamos cientistas de coração e gostemos de aprender coisas novas e desafiadoras, não corremos atrás de modismos.

Muitas vezes há pressão para evitar novas tecnologias, como ao lidar com regulamentações, compliance, explicabilidade e outros requisitos em serviços financeiros e em diversos outros setores com os quais trabalhamos nos EUA, no Reino Unido ou na Europa, por exemplo. Manter o status quo também envolve muito menos risco e trabalho, mas nos prende ao passado. Concluimos que adotar a IA valia a pena para aumentar o valor das nossas soluções sem comprometer sua integridade.

O motivo de usarmos IA é simples. Na busca incessante por fazer melhor – seja detectando mais fraudes, gerando menos atrito para bons consumidores, apoiando melhor as pessoas financeiramente excluídas ou garantindo que nossos produtos não tenham vieses –, a IA oferece um rico conjunto de métodos. Esses métodos ampliam nossa capacidade de obter novos insights e produzir melhores resultados, acompanhando a velocidade, o ritmo e a complexidade dos negócios dos nossos clientes.

Embora a IA e a IA generativa – a capacidade de computadores criarem conteúdo original a partir de um comando humano – ofereçam capacidade e ferramentas para construir um processo melhor de proteção de identidade, a tecnologia também está sendo usada por fraudadores. A IA aumenta a eficiência e a escala dos ataques e dá origem a uma nova gama de golpes sofisticados de phishing, identidades sintéticas, roubo de identidade com “deepfake” e falsificação de documentos. Em outras palavras, a IA pode fortalecer tanto a prevenção a fraudes quanto a capacidade de atuação dos fraudadores.

A região da Ásia-Pacífico, em particular, registrou uma explosão de golpes com deepfake impulsionados por IA, com um aumento de mais de 1.500% nos casos de deepfake entre 2022 e 2023 – o segundo maior crescimento do mundo, atrás apenas da América do Norte.¹

Em um caso particularmente elaborado, um funcionário foi enganado por videochamadas com um deepfake do CFO, resultando na transferência fraudulenta de HK\$ 200 milhões para cinco contas bancárias.

Adotar a IA para o bem é crucial. Caso contrário, organizações legítimas ficarão em desvantagem estratégica no combate a agentes mal-intencionados.

Quem adota a IA obtém resultados expressivos. Três grandes clientes bancários da LexisNexis® Risk Solutions que adotaram nossos modelos de IA contra golpes e tomada de conta (ATO - Account Takeover) tiveram um impressionante aumento médio de 260% no valor das fraudes detectadas em relação aos sistemas existentes. Em termos monetários, são dezenas de milhões de dólares a mais protegidos por ano.

Você sabia?

São 11.000 tecnólogos inovando na RELX, nossa controladora listada no FTSE 100. Isso nos dá uma visão única dos riscos e do poder da IA em casos de uso e marcos regulatórios muito diversos.



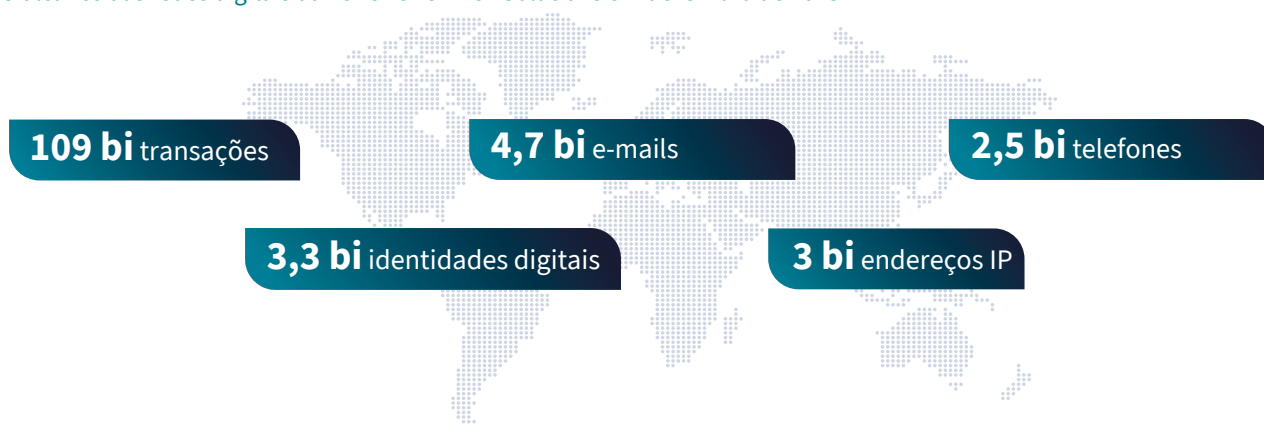
IA para ampliar o valor de grandes volumes de dados e aprimorar a detecção de fraudes

O volume e a complexidade dos dados continuam crescendo. Extrair os inúmeros insights valiosos que eles contêm e gerenciar sua enorme escala é uma tarefa desafiadora – mas que abraçamos com entusiasmo.

A LexisNexis® Risk Solutions tem uma das maiores redes de dados digitais e físicos do mundo. Nossa experiência em extrair insights e convertê-los em resultados tangíveis com IA é tão rica quanto nossos dados.

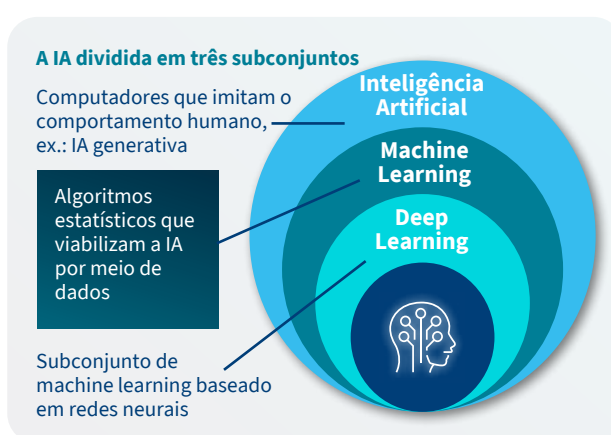
Nossas redes digitais globais crescem e geram mais insights a cada ano. Veja abaixo alguns dos principais números registrados.

O alcance das redes digitais da LexisNexis® Risk Solutions em dezembro de 2023



Usamos machine learning, um subconjunto da IA, para interpretar nossas redes, prever riscos e combater fraudes. São algoritmos estatísticos adequados para combinar e analisar enormes conjuntos de dados como os nossos e identificar sinais, padrões e relações relevantes para criar soluções práticas.

No entanto, é importante notar que a análise de fraudes não é padronizada. Usamos abordagens distintas para diferentes esquemas de fraude (primária vs. de terceiros vs. sintética), setores (telecom vs. cartão de crédito), modalidades (digital vs. física) e regiões.



Cada algoritmo é projetado para otimizar matematicamente a solução de um mesmo problema de maneiras diferentes, de modo que algoritmos distintos podem gerar insights distintos. Combinar essas técnicas com tamanho volume de dados é um ótimo começo, mas a única forma de realmente gerar valor é aliar ambos a um profundo conhecimento dos dados e expertise no assunto, com uma abordagem de governança de modelos e IA responsável.

Com esses elementos atuando em harmonia, criamos soluções que atendem às necessidades de negócio e de compliance de cada cliente e, em última instância, geram melhores resultados.

A busca contínua por melhores resultados para os clientes

A LexisNexis® Risk Solutions utiliza inteligência artificial para melhorar resultados há décadas. Está no nosso DNA.

Nosso primeiro uso de IA veio na aquisição da RiskWise International LLC em **2000**, quando a capacidade de crédito era avaliada com dados alternativos e um algoritmo de regressão logística em um produto chamado ThinDex™, antecessor do nosso conjunto de scores de risco de crédito LexisNexis® RiskView™.

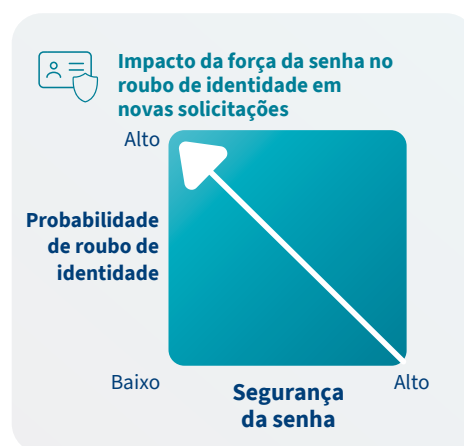
Os modelos de regressão logística estimam a probabilidade de um resultado binário e são úteis quando os dados são mais limitados ou quando a relação entre os dados e o resultado é linear. No caso do ThinDex, otimizamos algoritmos para ajudar instituições financeiras a incluir mais consumidores que talvez não pudessem ser pontuados pelas métricas tradicionais de crédito, com pouco ou nenhum impacto na exposição geral da instituição ao risco de perdas de crédito.

Por exemplo, os primeiros modelos RiskView™ detectaram que um volume maior de buscas recentes por crédito estava associado a uma probabilidade maior de inadimplência do que um volume menor.



A expansão para casos de uso de prevenção a fraudes veio logo em seguida, no início dos anos 2000. A ID Analytics, fundada em **2002** e adquirida pela LexisNexis® Risk Solutions em 2020, foi pioneira nesse campo. Foi uma das primeiras empresas a usar machine learning preditivo em consórcios de múltiplos credores, combinado à teoria dos grafos, para identificar redes de atividades fraudulentas e indivíduos envolvidos em fraudes.

A regressão logística não foi usada com eficácia apenas em consórcios de dados físicos: no mundo digital, ela também foi empregada com sucesso para detectar fraudes. Por exemplo, na LexisNexis® ThreatMetrix®, fundada em **2005** e adquirida pela LexisNexis® Risk Solutions em 2018, esses modelos de regressão logística identificaram uma associação entre o uso de uma senha insegura e uma maior probabilidade de roubo de identidade em uma nova solicitação.

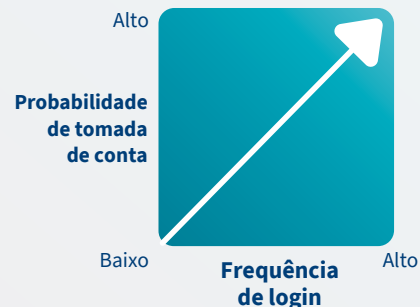


Os modelos também mostraram que um aumento de logins em um curto período, ou logins a partir de um local desconhecido, eram indicativos de tomada de conta (Account Takeover).

O poder da regressão logística está em sua capacidade de embasar decisões em tempo real, analisando milhares desses sinais de risco em um instante. Os modelos de regressão oferecem proteção aprimorada contra casos simples de fraude em todos os pontos de contato com o cliente, com implementação possível em questão de horas. Desde o primeiro uso desse método na LexisNexis® Risk Solutions, oferecemos diversos modelos “prontos para uso” de destaque, pré-configurados por setor, cenário de fraude e caso de uso, que oferecem prevenção instantânea a fraudes com mínima necessidade de gestão contínua.



Impacto da frequência de login na tomada de conta



Destaque:

Um grande varejista francês usou regressão logística para reconhecer clientes recorrentes e confiáveis, independentemente de quando e onde realizam transações. O resultado foi uma redução das tomadas de conta (Account Takeover) e das fraudes de pagamento, e a detecção de 95% das perdas potenciais por fraude.



Nossa principal prioridade é ajudar nossos bons clientes a fazer pedidos com segurança e sem o risco de terem suas contas comprometidas. Ao detectar atividades fraudulentas o mais cedo possível na jornada do cliente, a ThreatMetrix protege a integridade da nossa plataforma.”

Ampliando nossa capacidade de prevenir fraudes complexas com IA

Embora os modelos logísticos sejam mais preditivos que os sistemas baseados em regras e um ótimo ponto de partida para o uso de IA, às vezes a complexidade dos dados subjacentes exige uma abordagem diferente.

Como descrito na regressão logística, pressupõe-se que a relação entre as informações nos dados e a probabilidade de um resultado seja linear (ex.: alta variação de endereço = alto risco; baixa variação de endereço = baixo risco).

No entanto, as relações entre dados e resultados costumam ser mais complexas. Por exemplo, o histórico de um universitário com várias mudanças de endereço nos últimos dois anos pode ser perfeitamente normal, enquanto várias mudanças recentes de endereço de um proprietário de imóvel estabelecido há muito tempo podem não ser.

Em muitos casos, há uma interação entre o risco e o comportamento do consumidor – um contexto – que é capturado pelas variáveis dos dados. Como esse contexto é não linear, ele não pode ser totalmente capturado por modelos lineares.

Risco associado a mudanças de endereço e o contexto de “quem”



Estudante



Proprietário

Várias
mudanças de
endereço

Baixo

RISCO

Alto

Entendendo relações não lineares com árvores de decisão

Os fraudadores prosperam na complexidade, encontrando brechas e explorando-as. Por meio de experimentos no **início dos anos 2000**, logo percebemos que as árvores de decisão permitiam interações mais complexas entre os fatores nos dados, captando relações não lineares e melhorando a capacidade do modelo de prever um resultado.

Em resumo, árvores de decisão são algoritmos sofisticados que ajudam a identificar brechas e casos extremos que podem facilitar o trabalho dos fraudadores. Elas dividem os dados a cada etapa de modo a maximizar a diferença entre a população-alvo (ou seja, as fraudes) e o restante dos dados, até atingir um equilíbrio ideal entre o desempenho nos dados de treinamento e a capacidade de generalizar para novos conjuntos de dados. O objetivo é encapsular os dados de entrada na menor “árvore” possível e, assim, apresentar a previsão mais precisa.

Modelos do tipo árvore de decisão surgiram na ID Analytics® em **2008**, em um produto chamado ID Score®, e na LexisNexis® Risk Solutions por volta de 2011, em um produto então chamado LexisNexis® FraudPoint®. Ambos foram projetados para detectar fraudes de identidade na abertura de contas.

Combinando árvores de decisão para a máxima detecção de fraudes

Com o avanço do trabalho em nosso laboratório de ciência de dados, percebemos que poderíamos detectar fraudes ainda melhor com gradient boosting machines (GBM).

Enquanto um modelo de árvore de decisão tem uma única árvore, os GBMs contêm um grande número delas, construídas uma de cada vez, com otimização de falsos positivos e falsos negativos. Cada nova árvore analisa o erro das anteriores para prever melhor o que elas, coletivamente, erraram. Os resultados das árvores são combinados ao longo do processo para otimizar a solução, gerando um desempenho ainda melhor do modelo.

Já usávamos GBMs para detectar fraudes em **2009**, quando o poder computacional passou a permitir calcular um score em poucas centenas de milissegundos no ambiente de produção.

Ao comparar os GBMs com os modelos logísticos anteriores, todos os clientes que testamos inicialmente relataram algum ganho.

Em laboratório, colocamos os GBMs à prova contra vários outros métodos de IA, incluindo redes neurais, redes neurais convolucionais e máquinas de vetores de suporte. Em todos os casos até agora, os modelos GBM tiveram desempenho equivalente ao desses métodos mais sofisticados, sem sua complexidade computacional, alta exigência de dados e opacidade. Os modelos GBM podem ser explicados tanto a clientes quanto a consumidores. Por isso, as capacidades baseadas em GBM são um pilar do conjunto de ferramentas da LexisNexis® Risk Solutions e estão presentes em muitos dos nossos produtos, incluindo FraudPoint®, LexisNexis® Fraud Intelligence, ThreatMetrix®, LexisNexis® Emailage® e LexisNexis® BehavioSec®.

Os GBMs são modelos poderosos, flexíveis e explicáveis, que geram resultados consistentes para nossos clientes.

Estudo de caso: ganho médio do GBM vs. regressão logística, por setor



Estudo de caso: Grande banco combate golpes com cartão não presente usando GBMs

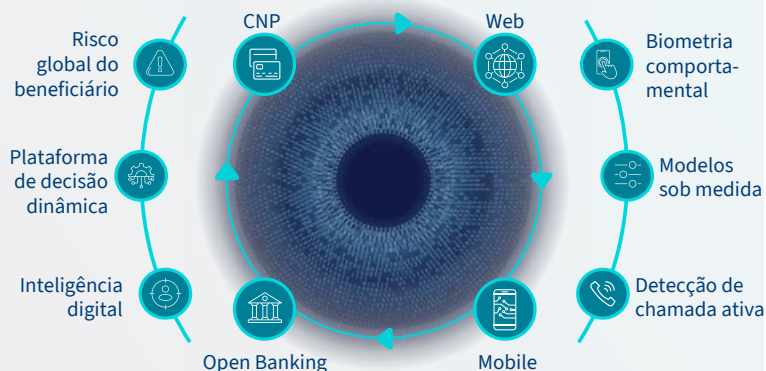
Na UE e no Reino Unido, a Autenticação Forte do Cliente (SCA) exige que as instituições financeiras usem dois de três fatores independentes para confirmar transações online: por exemplo, um fator de conhecimento (ex.: senha), de posse (ex.: dispositivo) e/ou de inerência (algo que caracteriza o usuário, como um atributo biométrico ou comportamental). Em vigor no Reino Unido desde 2022, a diretiva SCA reduziu em 15% as fraudes com cartão não presente (CNP).

Inevitavelmente, os fraudadores estão adaptando seus ataques. Crescem as táticas de engenharia social, em que fraudadores induzem clientes a autenticar transações fraudulentas com cartão no e-commerce.

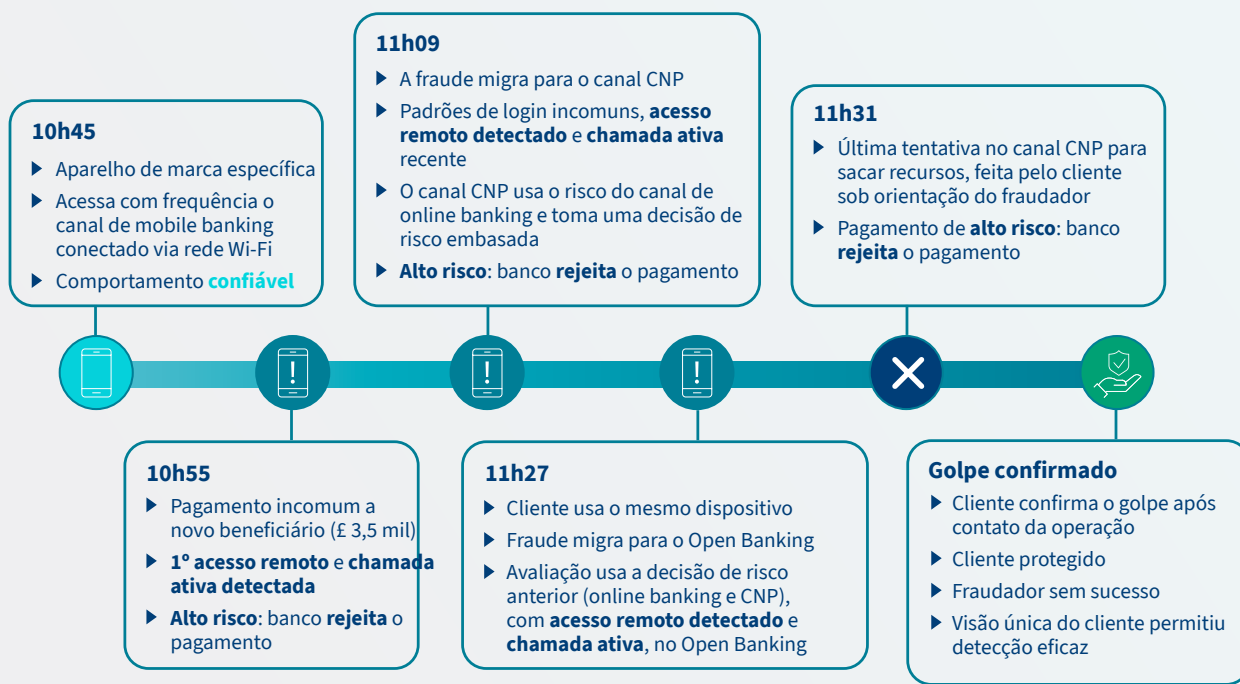
Um grande banco do Reino Unido respondeu usando GBMs para construir uma visão única e contextual do risco de golpes do cliente, com base em inteligência de online banking, mobile e open banking, e em ferramentas avançadas, como a detecção de chamadas ativas.

Isso interrompeu o ciclo da engenharia social e permitiu ao banco detectar **mais de US\$ 630 mil em fraudes em apenas vinte dias**. A linha do tempo abaixo mostra um exemplo da política em ação.

Visão contextual do risco de golpes nos canais de pagamento



Bloqueando golpes com cartão não presente em tempo real



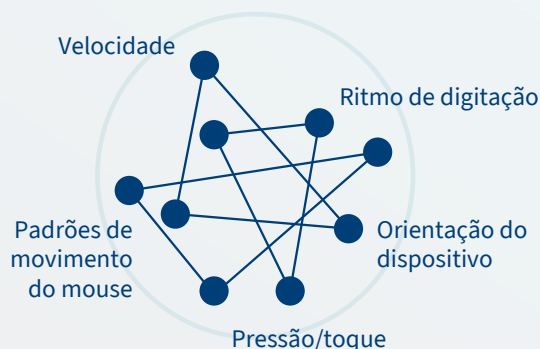
Detecção de fraudes com IA: não apenas para scores de risco

Ao longo dos anos, a LexisNexis® Risk Solutions incorporou uma série de capacidades adicionais de IA às nossas soluções, seja por meio de desenvolvimento interno ou de nossas diversas aquisições.

As técnicas de score de risco apresentadas até aqui usam machine learning “supervisionado”: técnicas de IA que usam uma função-alvo clara (ex.: fraudes confirmadas no seu negócio) para treinar os modelos e isolar padrões específicos de comportamento.

Também melhoramos resultados com machine learning “não supervisionado”, que utiliza algoritmos capazes de identificar padrões e insights sem dados previamente rotulados. Em geral, esses métodos agrupam padrões semelhantes ou detectam padrões anômalos. Por exemplo, o LexisNexis® BehavioSec® usa modelos não supervisionados para identificar irregularidades no comportamento biométrico do usuário em comparação a perfis construídos automaticamente ao longo do tempo, como a forma como o cliente interage fisicamente com um dispositivo. Esses elementos são um recurso de autenticação passiva muito usado na defesa contra fraudes de muitos clientes, sobretudo quando preservar a experiência do cliente é essencial.

Comportamentos do usuário que o BehavioSec avalia coletivamente com IA



O ThreatMetrix SmartID permitiu a um cliente de serviços financeiros ver o risco associado entre dispositivos e o número de contas de clientes acessadas:

Cliente de serviços financeiros identifica riscos com dados variados



Nossos modelos supervisionados e não supervisionados alimentam soluções que podem ser facilmente combinadas em camadas para oferecer o equilíbrio ideal entre risco e experiência para cada organização. Também experimentamos continuamente diversos algoritmos e modalidades de IA, usados para desenvolver novos produtos e extrair insights que nos ajudam a entender melhor os problemas enfrentados por nossos clientes.

O que esperamos que fique claro neste breve histórico do uso de IA na LexisNexis® Risk Solutions é que somos criteriosos em nossa abordagem. Antes de adotarmos um novo método de IA, ele precisa atender a três requisitos essenciais:

- 1) Deve ser adequado ao problema em questão;
- 2) Deve melhorar o resultado para nossos clientes;
- 3) Precisamos ser capazes de entender e explicar como o método funciona e o que ele está fazendo.

O que nos leva a outro tema central para nossa abordagem: responsabilidade.

Nosso compromisso com a IA responsável

A ascensão da IA generativa aumentou o senso de urgência nas discussões globais sobre os riscos da IA em diferentes casos de uso e sobre os parâmetros para seu uso responsável.

A LexisNexis® Risk Solutions, junto com nossos parceiros corporativos da RELX, participa ativamente dessas discussões. Embora os [princípios de IA responsável da RELX](#) tenham sido publicados em 2022, já atuávamos em sintonia com eles e debatíamos esses temas muitos anos antes.

Princípios de IA responsável da RELX

Entender o impacto
no mundo real

Respeitar a
privacidade e
fortalecer a
governança
de dados

**Nosso
compromisso
com a IA
responsável**

Evitar exclusão
e vieses

Tornar tudo
explicável e
responsabilizável

Acreditamos profundamente na missão por trás desses princípios e os compartilhamos em diversos fóruns, com públicos que incluem reguladores, defensores do consumidor e nossos clientes. Também publicamos white papers sobre [dados alternativos de crédito](#) e [inclusão financeira](#), ambos pilares da nossa missão.

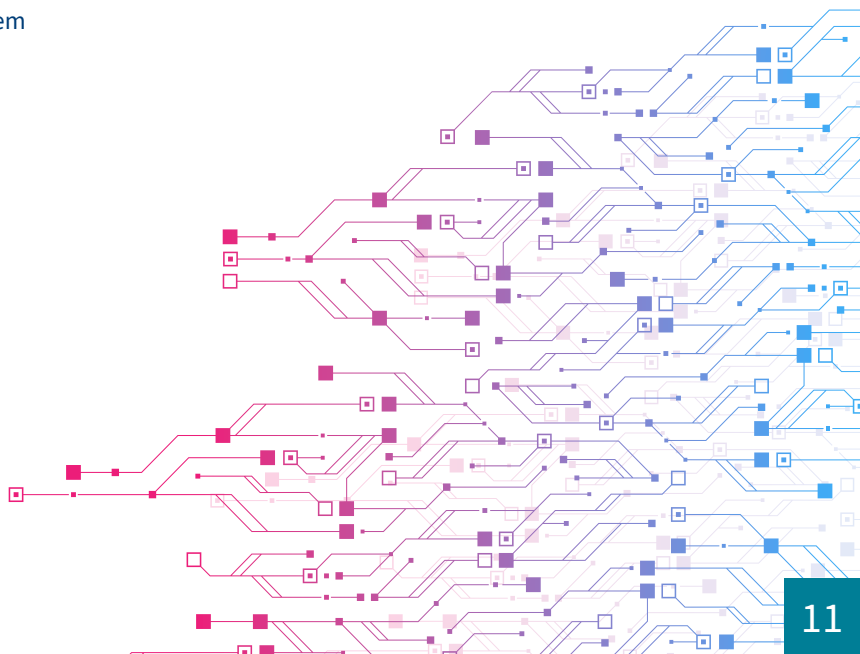
Também investimos em uma equipe global de cientistas de dados cuja função é entender o impacto das escolhas metodológicas tanto na eficácia dos produtos quanto em questões de crédito justo e vieses.

Compreender os fundamentos de um resultado modelado nos ajuda a melhorar continuamente a eficácia e a equidade dos modelos. Embora essa equipe seja tecnicamente responsável pela governança de modelos, nossos Princípios de IA da RELX têm uma definição ampla de modelos de IA, que “inclui quaisquer insights gerados por máquinas a partir das ferramentas e técnicas do campo da ciência de dados”. Na prática, essa equipe monitora desde sistemas baseados em regras até a IA generativa.

Nossos cientistas de dados ajudam clientes internos e externos a refletir sobre o que é necessário para governar novas tecnologias e como avaliá-las e monitorá-las quanto a desempenho ou vieses. Eles chegaram a desenvolver modificações no algoritmo GBM padrão para lidar melhor com condições nos dados que podem gerar vieses não intencionais.

Por exemplo, historicamente, a ausência de certas informações de identificação pessoal (ex.: o Social Security Number, nos EUA) seria automaticamente um indicador de risco mais alto em uma solicitação de abertura de conta. Com o tempo, porém, a crescente sensibilidade global à privacidade tem levado alguns clientes a não querer coletar, armazenar ou retransmitir certas informações. Esse algoritmo GBM modificado lida com populações sem determinada informação sem perder a capacidade de isolar a subpopulação genuinamente arriscada.

Nossos cientistas de dados também realizam sessões informativas com as equipes de gestão de risco de modelos dos clientes e podem fornecer documentação mediante solicitação, apoiando os processos internos de governança de modelos de cada cliente.



Ampliando suas possibilidades com a IA

Então, o que tudo isso significa para nossos clientes? E quais são nossos planos para o futuro?

Primeiro, a combinação dos nossos vastos e diversificados ativos de dados, de um rico conjunto de técnicas de IA, de um DNA de produtos pautado pela IA responsável e de profunda expertise setorial deve lhe dar confiança de que a LexisNexis® Risk Solutions é uma parceira para enfrentar desafios complexos de fraude e identidade.

Os exemplos deste documento são uma fração das muitas explorações de IA em nosso laboratório e das inúmeras histórias reais de uso da tecnologia para melhorar os resultados dos clientes. [Leia mais aqui \(Conteúdo em Inglês\).](#)

Segundo, e para concluir, vale falar de algumas das principais inovações baseadas em IA que estão por vir – todas com foco em oferecer ferramentas e tecnologia para gerenciar seus próprios modelos de IA e melhorar os resultados para seus clientes.



IA Self-Service torna os analistas de dados dos clientes tão poderosos quanto cientistas de dados. O ThreatMetrix é o primeiro produto do setor a colocar o controle total dos modelos de IA em suas mãos, com um portal self-service intuitivo para configurar seus próprios modelos com mínimo conhecimento de ciência de dados.



Fraud Genome Project, projeto parceiro da IA Híbrida, explora múltiplas abordagens de modelagem para classificar melhor os tipos de fraude nos dados de fraudes reportadas.

Ao sobrepor dados dos nossos consórcios às fraudes identificadas pelos clientes e aplicar diversos métodos de machine learning, vemos padrões de comportamento emergirem. Isso nos ajuda a agrupar as fraudes em perfis comportamentais e otimizar ainda mais os resultados.



IA Adaptativa aumentará o desempenho dos modelos ao permitir ajustes frequentes sem o pesado esforço de compliance normalmente associado às atualizações de modelos.



IA Generativa oferece poderosas capacidades de combate a fraudes. Estamos explorando seu uso como substituta da tradicional autenticação baseada em conhecimento (KBA) de múltipla escolha, que pode ter a consequência indesejada de fornecer ao fraudador respostas prováveis e revelar informações pessoais adicionais. Com a IA generativa, a KBA pode ser feita com respostas abertas em texto livre, o que a torna muito mais difícil de burlar. Também estamos explorando a capacidade da IA generativa de extrair informações de campos de texto livre que ajudem a avaliar o risco de uma transação.



IA Híbrida aumentará a eficácia da detecção de fraudes ao permitir que os clientes acionem individualmente um conjunto de modelos, cada um configurado para detectar um tipo diferente de fraude. A estrutura híbrida então determina qual dos modelos indica o maior risco e que tipo de fraude esse risco representa.

Considerações finais

A LexisNexis® Risk Solutions incorporou a IA como parte da nossa missão de proteger nossos clientes contra fraudes e ampliar as oportunidades para que todos os consumidores participem de forma segura e plena do ecossistema financeiro.

Continuaremos a mantê-lo informado sobre nossa busca por melhorar seus resultados e ajudá-lo a proteger cada interação com seus clientes. Esperamos trabalhar com você para resolver os desafios que seu negócio enfrenta hoje e se preparar para os que virão.

Se quiser saber mais sobre a tecnologia e os métodos discutidos neste documento ou sobre nossos planos futuros, nossos especialistas globais e locais estão à sua disposição.

Juntos, vamos proteger cada interação com o cliente.

Fale com seu representante da LexisNexis® Risk Solutions ou acesse risk.lexisnexis.com.br para saber mais.



A LexisNexis® Risk Solutions utiliza o poder dos dados e de análises avançadas para fornecer insights que ajudam empresas e entidades governamentais a reduzir riscos e tomar melhores decisões em benefício de pessoas em todo o mundo. Oferecemos soluções de dados e tecnologia para diversos setores, incluindo seguros, serviços financeiros, saúde e governo. Com sede na região metropolitana de Atlanta, Geórgia (EUA), temos escritórios em todo o mundo e fazemos parte da RELX (LSE: REL/NYSE: RELX), fornecedora global de ferramentas de análise e decisão baseadas em informação para clientes profissionais e empresariais. Para mais informações, acesse www.risk.lexisnexis.com e www.relx.com.

Nossas soluções ajudam organizações a prevenir crimes financeiros, alcançar conformidade regulatória, mitigar riscos de negócio, aumentar a eficiência operacional e ampliar a lucratividade.

Este documento tem caráter meramente informativo e não garante a funcionalidade ou os recursos de nenhum produto da LexisNexis Risk Solutions aqui identificado. A LexisNexis Risk Solutions não declara nem garante que este documento esteja completo ou livre de erros.

As definições de IA variam conforme a jurisdição, e as regulamentações ainda estão em desenvolvimento. Aqui, abordamos uma variedade de métodos, da matemática tradicional, como a regressão estatística, a tecnologias de IA, como a IA generativa e as redes neurais.

LexisNexis e o logotipo Knowledge Burst são marcas registradas da RELX Inc. ID Analytics, ID Score, FraudPoint, Accuity e Emailage são marcas registradas da LexisNexis Risk Solutions FL Inc. ThreatMetrix e ThreatMetrix SmartID são marcas registradas da ThreatMetrix, Inc. BehavioSec é marca registrada da Behaviometrics AB. RiskView e ThinDex são marcas da LexisNexis Risk Solutions Inc. RELX e o símbolo RE são marcas da RELX Group plc, usadas sob licença. Outros produtos ou serviços podem ser marcas ou marcas registradas de suas respectivas empresas.

Copyright © 2024 LexisNexis Risk Solutions.

Fontes

¹ <https://globalinitiative.net/analysis/deepfakes-ai-cyber-scam-south-east-asia-organized-crime/>

