JUN 2026

NEWSLETTER

Olhar Opice BLUM

EDITORIAL

Fraudes digitais cada vez mais sofisticadas têm colocado à prova a capacidade de reação das organizações, que precisam proteger seus ativos, preservar sua reputação e cumprir exigências regulatórias cada vez mais rigorosas. Em muitos casos, o prejuízo financeiro é só o primeiro impacto.

Os números ajudam a dimensionar o cenário. Nos nove primeiros meses de 2025, o Brasil registrou mais de 10,8 milhões de tentativas de fraude, um crescimento de 28,6% em relação ao mesmo período do ano anterior. O setor financeiro respondeu por mais da metade das ocorrências registradas, evidenciando o grau de exposição de empresas que operam em ambientes digitais e transacionais.

Nesse contexto, prevenir continua sendo essencial, mas já não é suficiente. A capacidade de investigar rapidamente o incidente, preservar evidências, recuperar valores, atender exigências regulatórias e coordenar uma resposta multidisciplinar virou um diferencial fundamental.

Nesta edição, analisamos as fraudes digitais sob diferentes perspectivas: a responsabilização e recuperação de prejuízos, a resposta a incidentes, os desafios regulatórios do sistema financeiro, os impactos para a proteção de dados, os riscos trazidos pela inteligência artificial, a proteção de marcas e ativos digitais, o papel dos processos internos na prevenção de fraudes e os reflexos tributários decorrentes de perdas financeiras. Não perca.

O Olhar Opice segue como espaço de análise crítica sobre temas que atravessam tecnologia, sociedade e negócios, sempre à luz do Direito Digital e das soluções que desenvolvemos no Opice Blum. Nosso compromisso é ampliar o seu repertório e mostrar como o jurídico pode contribuir para um ambiente digital mais seguro, ético e sustentável.

Fontes:

Serasa Experian. Brasil registrou 10,8 milhões de tentativas de fraude até setembro de 2025, com alta de 28,6%.

https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/brasil-registrou-108-milhoes-de-tentativas-de-fraudes-ate-setembro-com-alta-de-286-aponta-serasa-experian/

Serasa Experian. Quase 7 milhões de tentativas de fraude no primeiro semestre de 2025; setor bancário é o principal alvo.

https://www.serasaexperian.com.br/sala-de-imprensa/indicadores/recorde-quase-7-milhoes-de-tentativas-de-fraude-foram-registradas-no-1-semestre-de-2025-setor-bancario-e-principal-alvo/

SUMÁRIO

FRAUDES DIGITAIS E O NOVO DEVER DAS PLATAFORMAS

As fraudes digitais vão muito além dos prejuízos financeiros. Hoje, golpes praticados por meio de perfis falsos, anúncios fraudulentos, páginas que utilizam marcas de terceiros, contas inautênticas e campanhas coordenadas de desinformação exigem respostas rápidas para evitar a ampliação dos danos.

Nesse cenário, o recente julgamento do STF sobre o Marco Civil da Internet que finalizou na última semana, trouxe mudanças relevantes para a atuação contenciosa. A Corte passou a admitir, em diversas hipóteses, a responsabilização de plataformas que, após notificadas sobre conteúdos ilícitos, deixem de adotar providências adequadas para sua remoção. Também estabeleceu regime mais rigoroso para anúncios impulsionados, conteúdos patrocinados e os chamados virais, justamente porque são os frequentemente explorados por fraudadores, para alcançar a maior quantidade de vítimas no menor tempo possível.

Na prática, a discussão deixa de se concentrar Exclusivamente na indenização após o dano ou o golpe e passa a envolver mecanismos de contenção e repressão em tempo real. Medidas de remoção e bloqueio de perfis falsos ganham ainda mais relevância. A atuação jurídica também inclui a preservação de evidências digitais e identificação de responsáveis via quebra de sigilo.

Para empresas vítimas de fraudes, a estratégia jurídica combinar prevenção, investigação e atuação rápida especialmente perante plataformas digitais. Em um ambiente digital onde os danos se propagam em minutos, a velocidade da resposta tornou-se tão importante quanto a própria responsabilização.

Opice CAST

CONVERSAS QUE VÃO ALÉM DO ÓBVIO

Acompanhar o futuro digital exige conversas francas e contínuas.

Por isso, criamos **Opice Cast**, o videocast do Opice Blum que reúne sócios do escritório e convidados para discutir as transformações que estão redefinindo empresas, mercados e relações digitais.

Inteligência artificial, cibersegurança, proteção de dados, novas regulações, inovação e tendências tecnológicas são alguns dos temas tratados. Não perca.

Ouça no Spotify | Assista no YouTube

Opice BLUM

Redefinindo os limites do possível.

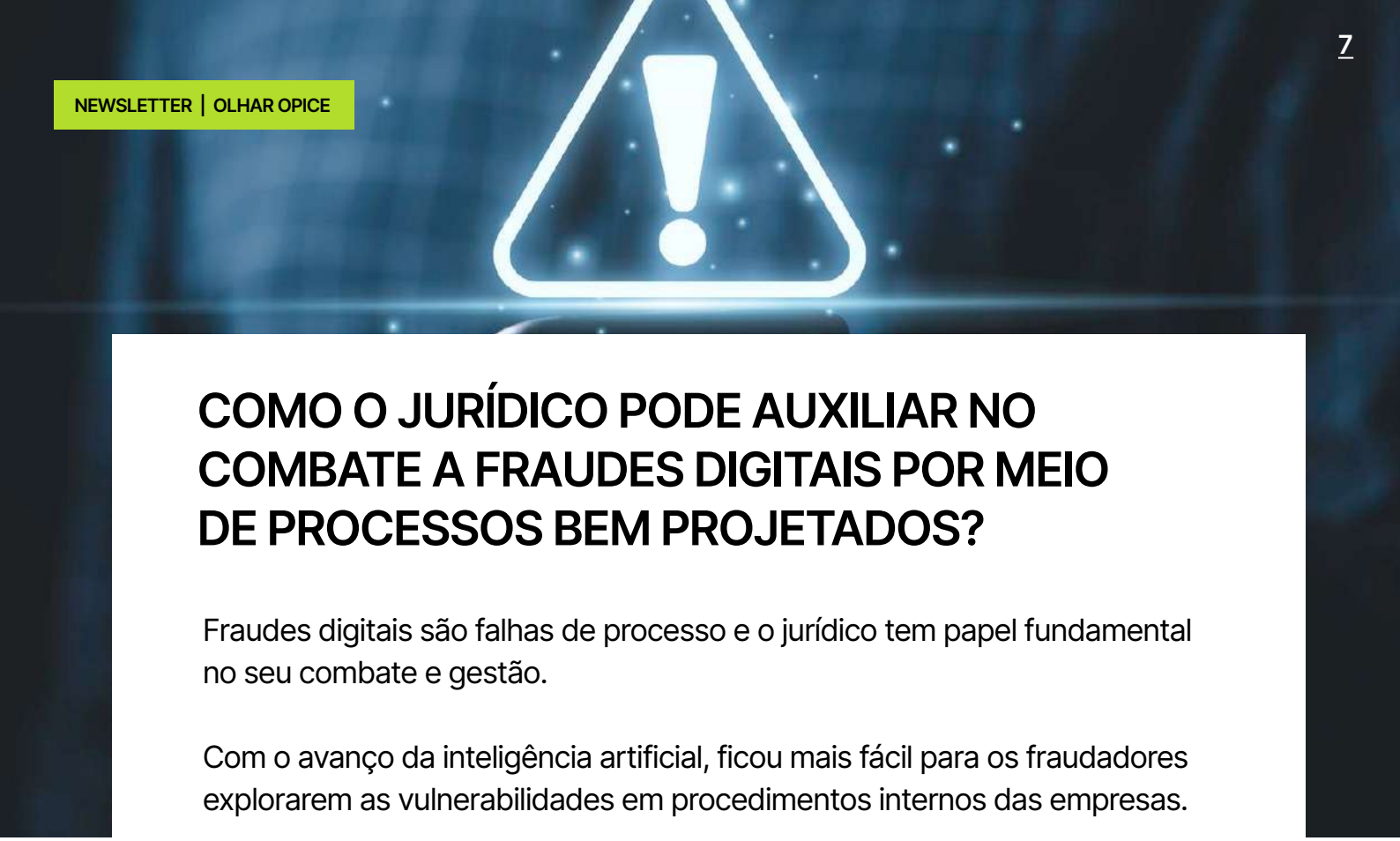
GOVERNANÇA DE IA COMO ALIADA NO COMBATE A FRAUDES

A inteligência artificial reconfigurou os dois lados da fraude digital. Se, por um lado, ela potencializa golpes como *deepfakes* que clonam vozes de executivos, engenharia social automatizada e identidades sintéticas indetectáveis a olho nu, por outro tornou-se a principal aliada na detecção de anomalias e na resposta a incidentes em tempo real.

O problema é que adotar IA sem governança só desloca o risco. Modelos treinados com dados enviesados, decisões automatizadas sem rastreabilidade e ausência de supervisão humana podem gerar falsos positivos, bloqueios indevidos e, sobretudo, dificultar a preservação de evidências e o atendimento a exigências regulatórias quando o incidente acontece.

É aqui que governança de IA e prevenção a fraudes se encontram, já que estruturas claras de responsabilização, documentação de modelos, controle de qualidade dos dados e mecanismos de auditoria são o que permite investigar com rapidez, sustentar a recuperação de prejuízos e demonstrar diligência diante de autoridades.

Em um cenário de 10,8 milhões de tentativas de fraude só até setembro de 2025, a pergunta é como, com que controles, sob qual responsabilidade e com qual capacidade de prestar contas cada organização usará IA.



COMO O JURÍDICO PODE AUXILIAR NO COMBATE A FRAUDES DIGITAIS POR MEIO DE PROCESSOS BEM PROJETADOS?

Fraudes digitais são falhas de processo e o jurídico tem papel fundamental no seu combate e gestão.

Com o avanço da inteligência artificial, ficou mais fácil para os fraudadores explorarem as vulnerabilidades em procedimentos internos das empresas.

Para ilustrar a situação, vale lembrar o caso de *voice phishing* no qual os criminosos clonaram a voz do CEO de uma empresa alemã para solicitar uma transferência financeira e o colaborador atendeu, enviando cerca de $243.000 para uma conta bancária na Hungria.

Depois do ocorrido é fácil afirmar que houve falha no processo do financeiro, que deveria ter havido algum tipo de validação e que faltou integração com outras áreas. No entanto, isso precisa ser pensado com antecedência.

O jurídico, em colaboração com TI, segurança da informação e outras áreas da empresa devem fazer isso em conjunto.

O jurídico deve, por exemplo, orientar sobre a proteção contratual e cláusulas de prevenção, sobre questões regulatórias envolvidas (como a relação com a ANPD no vazamento de dados pessoais) e sobre a preservação das evidências.

Por fim, o jurídico deve atuar na orquestração entre as áreas envolvidas, uma vez que a fraude reside no vão entre elas e a resposta final, como a análise de responsabilização, o acionamento do seguro e a judicialização.

Uma área de Legal Operations bem estruturada pode ajudar no desenho dos processos e controles, bem como na abordagem integrada do tema.

FRAUDES DIGITAIS E CONTRATOS ELETRÔNICOS: O QUE AS EMPRESAS DEVEM APRENDER COM O RECENTE POSICIONAMENTO DO STJ

A transformação digital trouxe inegáveis ganhos de eficiência para a formalização de negócios. Hoje, celebramos contratos em poucos cliques, aceitamos termos de adesão remotamente e as assinaturas eletrônicas se tornaram parte da rotina de empresas dos mais diversos setores. Porém, paralelamente, aumentaram os questionamentos judiciais relacionados a alegações de fraude em contratações feitas em ambiente digital.

Nesse contexto, merece destaque o recente posicionamento do Superior Tribunal de Justiça (STJ), que reconheceu a validade de contrato de empréstimo firmado por meio de plataforma de assinatura eletrônica não certificada pela Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil).

No julgamento do REsp nº 2.197.156/SP1, a Terceira Turma do STJ entendeu, por unanimidade, que a ausência de certificação ICP-Brasil, por si só, não é suficiente para invalidar a contratação eletrônica. A Corte considerou relevante o conjunto de evidências produzido durante a contratação, como o envio de documentos pessoais, a fotografia do contratante e os demais elementos aptos a demonstrar a manifestação de vontade e a autenticidade da operação.

A decisão reforça uma mudança importante de perspectiva: o principal risco jurídico das contratações eletrônicas decorre da fragilidade do processo de formalização adotado pela empresa e não da utilização desta ou daquela tecnologia de assinatura.

Em outras palavras, a discussão não é mais se a assinatura eletrônica é válida. A preocupação passou a ser se a organização possui mecanismos capazes de demonstrar, de forma consistente, quem realizou a contratação, quais etapas de autenticação foram percorridas e quais evidências foram preservadas para uma eventual utilização em juízo.

Nesse cenário, assumem papel central na mitigação de riscos as trilhas de auditoria robustas, a autenticação multifator, o registro de logs, a coleta adequada de evidências eletrônicas, a validação documental e os mecanismos de prevenção a fraudes.

A própria legislação brasileira já admite diferentes modalidades de assinatura eletrônica. O artigo 10, § 2º, da Medida Provisória nº 2.200-2/2001 estabelece que outros meios de comprovação da autoria e integridade de documentos eletrônicos podem ser admitidos, desde que aceitos pelas partes ou pela pessoa a quem o documento for oposto. Posteriormente, a Lei nº 14.063/2020 consolidou a classificação das assinaturas eletrônicas em simples, avançadas e qualificadas, reconhecendo distintos níveis de confiabilidade conforme a natureza do ato praticado.

Diante do crescimento das fraudes digitais e do aumento da judicialização envolvendo contratações eletrônicas, a revisão periódica dos fluxos de formalização se tornou uma iniciativa de governança, voltada à redução de contingências, ao fortalecimento da segurança jurídica e à proteção da reputação empresarial.

A FRAUDE SE CONSTRÓI ANTES DO GOLPE.

Fraudes digitais raramente começam no momento do golpe. Na maioria das vezes, são as informações e dados pessoais obtidos em contextos de incidentes de segurança que viabilizam esquemas sofisticados de engenharia social, abertura de contas fraudulentas, invasões de perfis, sequestro de credenciais e transações não autorizadas.

A exposição de dados cadastrais simples como CPF, telefone, e-mail, e até informações financeiras e padrões de comportamento, permitem que criminosos construam abordagens altamente convincentes, hoje potencializadas pelo uso de ferramentas de inteligência artificial, clonagem de voz e *deepfakes*.

Nesse cenário, proteger os dados pessoais é ainda mais estratégico para a contenção de fraudes. A adoção de medidas de segurança adequadas, controles de acesso, autenticação multifator, monitoramento contínuo e programas efetivos de governança, além da conformidade regulatória, permite reduzir a superfície de exposição e fortalecer a capacidade de resposta das organizações.

Além dos impactos financeiros e reputacionais, os incidentes de segurança podem gerar obrigações regulatórias perante a ANPD e titulares de dados, além de aumentar a exposição a litígios e responsabilização civil. No Brasil, o roubo de credenciais e a engenharia social já figuram entre os incidentes mais comunicados à ANPD.

A correlação entre vazamentos de dados pessoais e fraudes hoje é mensurável. Segundo o Verizon DBIR 2025, o abuso de credenciais foi vetor de acesso inicial em 22% das violações e 88% dos ataques a aplicações web envolveram credenciais roubadas. Enquanto a discussão se concentra no instante do golpe, é nos meses anteriores, durante o controle sobre quais dados circulam e por quanto tempo, que a fraude é sendo decidida. Cada base de dados pessoais protegida é um elo a menos na cadeia e é nesse momento que a fraude se torna evitável.

Fontes:
ANPD - Comunicações de Incidentes de Segurança (2025)
Página oficial e painéis interativos:
https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

Verizon, 2025 Data Breach Investigations Report
Relatório oficial (PDF): https://www.verizon.com/business/resources/Tea/reports/2025-dbir-data-breach-investigations-report.pdf
Página principal do DBIR: https://www.verizon.com/business/resources/reports/dbir/

QUANDO A MARCA DA EMPRESA VIRA FERRAMENTA DE FRAUDE CONTRA SEUS CLIENTES

Criminosos nem sempre precisam criar confiança nas vítimas do zero: eles podem simplesmente tomar emprestada a confiança dos clientes na marca.

Domínios falsos, perfis clonados e aplicativos fraudulentos que imitam marcas conhecidas são hoje ferramentas-padrão de engenharia social. Quanto mais reconhecida e admirada for a marca, maior a taxa de conversão do golpe. E assim, a imagem que a empresa levou anos para construir e consolidar se torna o principal vetor de ataque contra os seus próprios clientes.

O problema vai além da reputação. Há responsabilidade potencial por danos sofridos pelos consumidores enganados, especialmente se a empresa não tomar medidas tempestivas para mitigar os danos. Isso, sem mencionar a erosão do valor da marca, que pode passar a ser associada a ambientes pouco seguros.

O ordenamento jurídico oferece soluções, mas a velocidade na resposta é a chave. Entre as respostas possíveis, temos a remoção de conteúdo e produtos falsos por notificação direta às plataformas, a recuperação de domínios via disputa arbitral, as medidas cautelares de urgência e os registros preventivos de marcas e nomes de domínio, entre outras medidas possíveis. O que faz diferença é ter uma estratégia antes de precisar dela.

FRAUDES DIGITAIS E O NOVO FOCO REGULATÓRIO DO BANCO CENTRAL DO BRASIL

A expansão dos canais digitais, dos pagamentos instantâneos e a crescente sofisticação dos criminosos têm elevado os riscos de fraudes digitais para consumidores, instituições supervisionadas e fornecedores que integram o ecossistema.

Ao longo de 2025, os incidentes registrados evidenciaram que a exploração de vulnerabilidades em terceiros expande os riscos para além dos ambientes internos das instituições financeiras, o que reforçou a preocupação do órgão regulador com a resiliência operacional e a segurança das instituições.

Nesse contexto, o Banco Central do Brasil intensificou sua atuação regulatória e supervisora. Além do aprimoramento das medidas de prevenção a fraudes no ecossistema Pix, o regulador avançou na implementação de novos requisitos de segurança cibernética, reforçando expectativas relacionadas à governança, gestão de riscos, monitoramento contínuo, gestão de terceiros e resposta a incidentes.

A prevenção a fraudes e a segurança cibernética agora ocupam uma posição central nas estratégias de governança e conformidade. Afinal, a capacidade de identificar vulnerabilidades e responder tempestivamente a incidentes é essencial para a preservação da confiança e da segurança do sistema financeiro.

IDENTIDADE EMPRESARIAL, CNPJ E FRAUDE FISCAL DIGITAL

No ambiente dos crimes fiscais, as fraudes evoluem mais rapidamente do que os mecanismos de controle. Com a crescente digitalização, o CNPJ passou a ocupar posição central na identidade empresarial e, quando indevidamente acessado, torna-se porta de entrada para o uso ilícito de dados cadastrais e para fraudes fiscais e financeiras on-line.

Nos últimos anos, diversas operações revelaram esquemas estruturados baseados em tecnologia. Exemplo emblemático foi a Operação Retificadora, iniciada em 2022 e estendida até 2024 pela Receita Federal, Ministério Público e Polícia Federal. Falsos consultores tributários, com acesso eletrônico indevido a dados de empresas do Simples Nacional, pleiteavam restituições fraudulentas e se apropriavam dos valores, gerando prejuízos milionários. Neste contexto, a Receita Federal vem ampliando o uso da inteligência artificial para monitoramento, fiscalização e detecção de fraude, sonegação, inadimplência, bem como para identificar e beneficiar os bons pagadores.

Como resposta a essa vulnerabilidade, a Reforma Tributária aposta no **Split Payment, mecanismo que automatiza a retenção e o repasse automático do tributo no momento do pagamento, buscando justamente mitigar riscos de fraudes digitais**. Ainda assim, a rápida evolução das IAs e a incerteza quanto às novas normas de segurança exigem das empresas, investimentos contínuos em governança, compliance, proteção de certificados digitais e monitoramento das informações atreladas ao CNPJ.

Fontes:
Receita Federal inicia terceira etapa da Operação Retificadora, voltada para as empresas optantes pelo Simples Nacional — Receita Federal
Receita Federal publica Política de Inteligência Artificial com foco em responsabilidade, transparência e supervisão humana — Receita Federal
https://www.gov.br/fazenda/pt-br/assuntos/noticias/2024/maio/regulamentacao-foi-desenhada-para-evitar-fraudes-e-beneficiar-bons-pagadores-afirma-appy

PARA APROFUNDAR

Neste **guia de consulta rápida**, especialistas do Opice Blum compartilham aprendizados sobre prevenção, investigação digital, recuperação de valores, gestão de crise e resposta regulatória, reunindo experiências reais das áreas de Contencioso Digital, Inovação em Serviços Financeiros e Resposta a Incidentes. Um guia para entender o que fazer antes, durante e depois de uma fraude.

BAIXE AQUI

FORA DA LEI

Esta coluna é um espaço para olhar além do jurídico e explorar a expansão das bets sob uma lente mais social, cultural e antropológica. Nela, o foco está nos comportamentos, hábitos e transformações que a tecnologia provoca em nosso jeito de pensar.

O QUE VEM ANTES? O CLIQUE OU A FRAUDE?

As fraudes digitais costumam ser tratadas como problema de tecnologia, mas para as pessoas físicas, elas começam muito antes. Começam na pressa, na solidão, na promessa de vantagem, na autoridade falsa de uma mensagem bem escrita. Os golpes exploram falhas humanas, tanto quanto falhas de sistema.

Os dados ajudam a dimensionar o problema. Uma pesquisa do Fórum Brasileiro de Segurança Pública e do Datafolha apontou que 1 em cada 3 brasileiros sofreu fraude digital com prejuízo financeiro. O Anuário Brasileiro de Segurança Pública também mostrou alta de 17% nos casos de estelionato eletrônico em 2024.

O cenário revela que o fraudador hoje faz as vezes de bancos, empresas, familiares, plataformas, entregadores, atendentes e até vozes conhecidas. Ele entende o comportamento, explora a urgência e usa a tecnologia para parecer confiável.

A consequência é que a fraude digital nos coloca em estado de desconfiança permanente. Afinal, qualquer mensagem pode ser falsa, qualquer link pode ser armadilha e qualquer voz pode ser clonada.

Isso não significa que estamos condenados a viver sob suspeita. Ao longo da história, sempre que novas tecnologias alteraram as formas de interação, desenvolvemos mecanismos para restaurar a confiança. Foi assim com a popularização do papel-moeda, que exigiu sistemas de autenticação para combater falsificações; foi assim também com o comércio eletrônico, que levou à criação de certificados digitais e meios seguros de pagamento. O desafio contemporâneo talvez seja justamente esse: construir novas referências de autenticidade, verificação e reputação para um mundo em que nem tudo que parece verdadeiro é real.

Fontes:
Fórum Brasileiro de Segurança Pública e Datafolha.
Anuário Brasileiro de Segurança Pública 2025.

INSIGHTS DO FUTURO

Esta coluna é um espaço dedicado a discutir tendências que já começam a impactar o Direito, os negócios e a sociedade. Nesta edição, você lê como a IA está alterando a natureza das fraudes e por que a capacidade de detectar comportamentos suspeitos pode se tornar tão importante quanto a de impedir ataques.

FRAUDE COM IA: A PERGUNTA NÃO É MAIS QUEM ROUBOU, MAS QUEM DEVERIA TER VISTO

As fraudes financeiras no Brasil entraram em outra escala. Só os golpes via Pix custaram R$ 4,9 bilhões em 2025, o volume de golpes digitais cresceu 35%, e 42% dos brasileiros já sofreram perda financeira direta. A leitura corrente que trata o problema como questão de segurança - mais antifraude, mais autenticação - é insuficiente.

O que mudou foi o atacante. Segundo dados da Polícia Federal, 42,5% das fraudes financeiras no país já empregam inteligência artificial, e o uso de deepfakes cresceu 830% entre 2024 e 2025. Vozes e rostos clonados simulam executivos e gerentes. Em Hong Kong, uma videoconferência falsa levou um funcionário a transferir US$ 25 milhões em 2024. A natureza dos golpes passou a ser comportamental.

O deslocamento que o gestor de risco não pode ignorar é jurídico! À medida que a fraude fica indistinguível, o Judiciário troca a pergunta "quem aplicou o golpe" por "quem deveria tê-lo detectado". Tribunais já analisam caso a caso se a instituição falhou ao não bloquear movimentações atípicas. A conta migra para quem tinha o dever de ver, e não viu.

A OCDE nomeia a fraude digital como o principal risco apontado por 85% das jurisdições. Contra um ataque comportamental, a defesa é igualmente comportamental: cultura de verificação, confirmação por outro canal, processo desenhado para promover questionamentos. Treinar a equipe para desconfiar de uma ordem urgente protege mais que qualquer filtro. Ou seja, quem tratar fraude como linha de orçamento de TI vai descobrir que ela virou questão de governança.

Ricardo Nery, DPO e advogado especialista em Privacidade, Proteção de Dados e Inteligência Artificial.

Fontes:
[1] Correio Braziliense | https://www.correiobraziliense.com.br/economia/2026/04/7406124-perdas-com-deepfake-custam-uss-2-bilhoes.html | abr/2026

[2] SEGS | https://www.segs.com.br/seguros/447658-empresas-e-bancos-enfrentam-novos-desafios-com-avanco-de-deepfakes-e-golpes-de-ia | mai/2026

[3] ECO | https://eco.sapo.pt/especiais/deepfakes-ia-e-burloes-sao-o-novo-pesadelo-do-seu-dinheiro/ | mar/2026

[4] arXiv | https://arxiv.org/pdf/2601.08674 | 2026

PARA DISTRAIR

FILMES

PRIVACIDADE HACKEADA
Esse documentário de 2019 detalha o escândalo global envolvendo o Facebook e a empresa de consultoria política, Cambridge Analytica. Relembre como os dados pessoais de mais de 87 milhões de usuários foram coletados sem consentimento e transformados em armas políticas de manipulação em massa. Pertinente em ano de eleição.

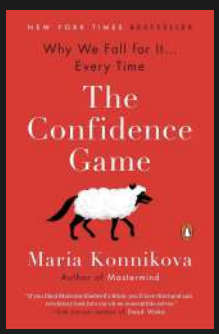
Disponível na Netflix.

SÉRIES

TERRA DE ILUSÕES:
INTERNET, MORTE E MENTIRAS
Esse documentário investigativo com 6 episódios não relacionados entre si aborda teorias da conspiração, ataques hacker, extorsão sexual, discurso de ódio, ligações falsas feitas para a polícia, entre outros. Um choque de realidade.

Disponível na Netflix.

LIVROS



THE CONFIDENCE GAME:
WHY WE FALL FOR IT... EVERY TIME!
Este livro de Maria Konnikova é uma ótima pedida para entender por que as pessoas caem em golpes. Aqui, o foco sai da tecnologia e vai para os mecanismos psicológicos mais explorados pelos fraudadores.

Disponível na Amazon,
ainda sem tradução para o português.

O OPICE BLUM NA MÍDIA EM JUNHO

Em reportagem publicada pela revista Veja, **Danielle Serafino**, sócia do Opice Blum Advogados, comenta os impactos da inteligência artificial no sistema de Justiça e os desafios éticos que acompanham sua adoção. Segundo ela, diante do aumento do uso de ferramentas de IA em processos judiciais, torna-se essencial reforçar mecanismos de verificação e segurança para identificar possíveis manipulações em documentos e garantir a confiabilidade das informações utilizadas por magistrados e advogados.

Em artigo publicado pela IAPP, **Henrique Fabretti**, CEO e sócio do Opice Blum Advogados, analisa os principais movimentos regulatórios da América Latina, destacando os avanços institucionais em países como Brasil, Peru e Chile, além dos desafios emergentes relacionados à inteligência artificial. Segundo ele, o cenário reforça a necessidade de uma governança mais estruturada e de uma atuação preventiva das organizações diante dos novos riscos tecnológicos e regulatórios.

Em artigo publicado na Cryptoid, **Camila Jimene**, sócia do Opice Blum Advogados, analisa os impactos da decisão do STF sobre a responsabilidade das plataformas digitais por conteúdos de terceiros. Segundo Camila, as mudanças na interpretação do artigo 19 do Marco Civil da Internet, destacando a ampliação dos deveres das plataformas na moderação e remoção de conteúdos ilícitos, além dos desafios regulatórios que a decisão traz para o ambiente digital no Brasil.

Renato Opice Blum,sócio-fundador e chairman do Opice Blum Advogados foi reconhecido como **Top Voice** no LinkedIn, distinção concedida a profissionais que se destacam pela produção de conteúdo relevante e pela contribuição qualificada para debates na plataforma. O reconhecimento reforça sua intensa atuação em temas relacionados ao Direito Digital, tecnologia, proteção de dados e inovação, contribuindo para a disseminação de conhecimento.

EXPEDIENTE

Contribuíram para esta edição:

Camilla Jimene, sócia de Contencioso Digital
Danielle Serafino, sócia de Legal X
Florence Terada, sócia de Tecnologia, Mídia e Entretenimento
Henrique Fabretti, CEO e sócio de Inteligência Artificial, Privacidade e Proteção de Dados, Resposta a Incidentes de Cibersegurança
Marcos Bruno, sócio de Tecnologia, Mídia e Entretenimento, Inovação em Serviços Financeiros e Propriedade Intelectual
Renato Opice Blum, sócio-fundador e chairman
Tiago Neves Furtado, sócio de Inteligência Artificial, Privacidade, Proteção de Dados e Resposta a Incidentes de Cibersegurança

Beatriz Vicente, team leader de Tecnologia, Mídia e Entretenimento
Bruno Blum Fonseca, advogado de propriedade Intelectual, Tecnologia, Mídia e Entretenimento
Camila de Araújo Guimarães, team leader de Privacidade, Proteção de Dados e Inteligência Artificial
Daniela Andrade, advogada de Tributário Digital
Gabriela Silveira Bueno dos Santos, team leader de Privacidade, Proteção de Dados e Inteligência Artificial
Laura Oliveira Spitzkopf, advogada de Tributário Digital
Mauro Roberto Martins Jr., advogado consultor de LegalX
Marina de Oliveira e Costa, team leader de Contencioso Digital
Pedro Figueiredo Soares, advogado de Inovação em Serviços Financeiros
Ricardo Nery, DPO e advogado de Privacidade, Proteção de Dados e Inteligência Artificial
Vivianne Prota, team leader de Inovação em Serviços Financeiros
Juliana Geve, Marketing
Gabriela Dias, Marketing
Sidney Marcos Filho, Designer

Se você gostou dessa edição do Olhar Opice, compartilhe com alguém que também pode apreciar o conteúdo. Até o mês que vem!