JUL 2026

NEWSLETTER

Olhar Opice BLUM

EDITORIAL

COMO PROVAR QUE ALGO É VERDADEIRO QUANDO TUDO PODE SER FALSIFICADO?

Durante muito tempo, bastava ver para acreditar. Uma fotografia servia como prova; uma voz identificava uma pessoa; um documento assinado era garantia de autenticidade. Hoje, nada disso é certeza.

O avanço da inteligência artificial tornou mais fácil, rápido e barato produzir imagens, vozes, documentos e vídeos impossíveis de distinguir dos originais. Ao mesmo tempo, as fraudes digitais, perfis e conteúdos falsos multiplicam situações em que verdade e não-verdade se confundem. A consequência é que **vivemos uma verdadeira crise de confiança**.

Essa transformação já alcança empresas, governos e tribunais. É preciso rever processos de autenticação, fortalecer mecanismos de verificação e desenvolver novas formas de provar a legitimidade das informações. A confiança, que antes era presumida, passa a depender cada vez mais de evidências.

Nesta edição, exploramos esse novo momento sob diversas perspectivas. Falaremos nos desafios jurídicos da identidade digital, na proteção de dados em um cenário de autenticações cada vez mais sofisticadas, nos impactos da IA sobre a produção de provas, nos reflexos para o sistema financeiro, na proteção de marcas, nos riscos para empresas e nas tecnologias que tentam reconstruir a confiança no ambiente digital.

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 repertório e mostrar como o jurídico pode contribuir para um ambiente digital mais seguro, ético e sustentável.

SUMÁRIO

DEEPFAKES E O COLAPSO DA CONFIANÇA NA IDENTIDADE DIGITAL

A popularização de *deepfakes* de voz e imagem tornou mais frágil a validação de identidade baseada apenas em aparência, voz ou familiaridade. Em ambientes corporativos, esse risco alcança aprovações financeiras, alterações cadastrais, redefinição de credenciais e solicitações urgentes atribuídas a executivos, colegas ou fornecedores.

A detecção técnica de *deepfakes* ajuda, mas não deve ser tratada como prova isolada. A qualidade das falsificações evolui rapidamente, enquanto ferramentas de detecção podem gerar falsos positivos e falsos negativos. A resposta mais segura está na combinação de sinais, como origem da chamada, dispositivo utilizado, comportamento incomum, contexto da solicitação e divergências em padrões de linguagem ou rotina.

A validação de identidade precisa incorporar confirmação por canal independente, autenticação multifator, segregação de funções e limites de aprovação proporcionais ao risco. Solicitações fora do padrão, especialmente com pressão por urgência ou sigilo, devem passar por verificação adicional antes da execução.

As ameaças internas também podem explorar esse cenário. Colaboradores mal-intencionados, contas comprometidas ou terceiros com conhecimento da operação podem usar *deepfakes* para contornar controles e atribuir ordens falsas a pessoas com autoridade. Por isso, a segurança depende menos de reconhecer rostos e vozes e mais de processos verificáveis, revisão de exceções e monitoramento de comportamentos incompatíveis com o histórico esperado.

DIGITAL PRIVACY SUMMIT 2026

O encontro que é referência em Direito Digital no Brasil ganha uma nova dimensão. Em **28 de outubro**, o Digital Privacy Summit reúne especialistas, executivos e lideranças para um dia de debates sobre inteligência artificial, proteção de dados, inovação, cibersegurança e os desafios jurídicos da economia digital. Tudo com a curadoria cuidadosa do Opice Blum.

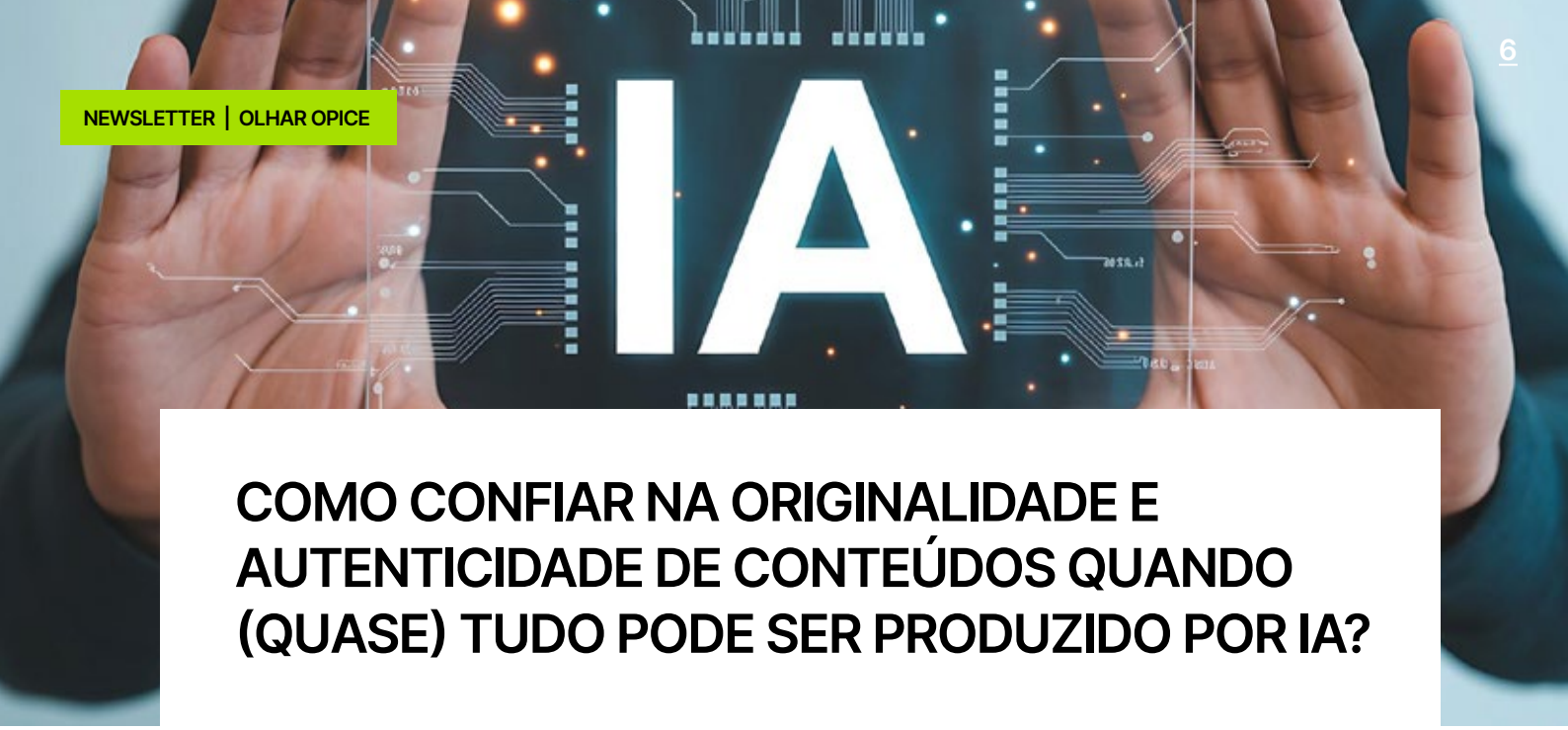
Adquira logo o seu ingresso para o Digital Privacy Summit. Se preferir, o Full Pass da Fenalaw dá acesso aos 3 dias do evento e também ao DPS.

10% de desconto com o cupom OPICEBLUM10 no checkout.

INSCREVA-SE AQUI

PROMOVIDO POR: Opice Blum FENALAW

APOIO: trustworks.



COMO CONFIAR NA ORIGINALIDADE E AUTENTICIDADE DE CONTEÚDOS QUANDO (QUASE) TUDO PODE SER PRODUZIDO POR IA?

Quando qualquer identidade e conteúdo podem ser sintetizados, replicados e reproduzidos em sistemas generativos, a governança de IA passa a envolver também a garantia da proveniência e originalidade do conteúdo, já que sem rastro verificável a autenticidade não consegue ser comprovada.

Watermarking (marca d'agua) e metadados de proveniência costumam ser apresentados como a resposta técnica ao problema. São úteis, mas frágeis, já que marcas podem ser removidas, metadados se perdem a cada recorte, compressão ou reencaminhamento, e nenhum detector tem precisão suficiente para sustentar sozinho uma decisão jurídica pela originalidade e legitimidade de um conteúdo.

Passa a ser necessário implementar controles de governança e documentação do processo criativo que, eventualmente, possam ser utilizados como meio de prova. A marcação de conteúdo sintético já aparece como obrigação no AI Act europeu e no PL 2338/2023, mas essa obrigação esparsa, sem cadeia de custódia, política interna e verificação nos pontos de decisão é apenas um rótulo, que pode não resolver todas as questões jurídicas de originalidade e autenticidade dos conteúdos sintéticos.

Com tudo isso, nasce a necessidade de contratos e processos de contratação que exijam declaração de origem do conteúdo gerado por IA. Esses processos devem ser compostos por trilhas de auditoria em fluxos críticos e por critérios explícitos sobre o que a organização considera suficiente para confiar no conteúdo apresentado. Também é fundamental estabelecer regras internas para a utilização desses conteúdos, garantindo a adequada prestação de contas.

QUANDO A IMAGEM CONTINUA TRABALHANDO SEM O INFLUENCIADOR

A inteligência artificial ampliou a escala e a gravidade do uso indevido da imagem. Fotografias, vídeos e áudios publicados por influenciadores e celebridades podem ser apropriados por terceiros, sem qualquer vínculo ou autorização, para criar conteúdos nos quais essas pessoas aparentemente recomendam produtos, defendem opiniões ou participam de situações que nunca ocorreram. **A questão jurídica central, portanto, não está só em distinguir o verdadeiro do falso, mas em impedir que a identidade de alguém seja transformada em matéria-prima para fraudes e manipulações.**

No Brasil, a imagem, a voz, a honra e a identidade são protegidas pelos direitos da personalidade. Ainda assim, os *deepfakes* desafiam a aplicação prática dessas garantias: o conteúdo pode ser produzido anonimamente, circular por diferentes plataformas e alcançar milhares de pessoas antes que a vítima consiga identificá-lo ou removê-lo. Além da violação individual, há impactos sobre consumidores e sobre o próprio mercado publicitário, pois a credibilidade construída pelo influenciador é artificialmente transferida para produtos, serviços ou discursos que ele nunca endossou.

A proibição de falsos depoimentos e endossos já aparece em iniciativas regulatórias estrangeiras, enquanto o AI Act europeu exige transparência para determinados conteúdos sintéticos. Porém, rotular um *deepfake* não legitima o uso não autorizado da identidade.

A única alternativa de resolução não pode continuar sendo deslocada para quem sofre a violação, como se a vítima tivesse condições reais de conter a velocidade e o alcance dessas práticas. Sobre isso, plataformas, anunciantes e intermediários precisam prever mecanismos de denúncia e remoção rápida, além de preservação de evidências.

É, ainda, necessário discutir a responsabilidade de quem cria, impulsiona ou obtém vantagem econômica com o conteúdo. Em uma crise de autenticidade é preciso identificar quem se apropriou daquela identidade e quem permitiu que ela circulasse como verdadeira.

COMO PROVAR A AUTENTICIDADE DE PROVAS DIGITAIS E CADEIA DE CUSTÓDIA

Em um cenário em que documentos, imagens, áudios e vídeos podem ser manipulados com facilidade, a discussão processual para alcançar como isso pode ser demonstrado em juízo.

A simples captura de tela, conhecida como *print*, por exemplo, nem sempre é suficiente para comprovar a autenticidade de um conteúdo digital. Cada vez mais, torna-se essencial preservar evidências de forma técnica, assegurando sua integridade e cadeia de custódia por meio de mecanismos como atas notariais, certificações digitais, *blockchains* e outras formas de preservação da prova.

Outro desafio crescente é a autoria. Na internet, quem aparenta ser o responsável por uma publicação nem sempre é quem efetivamente a produziu. Nesses casos, a identificação do autor pode depender de medidas judiciais de preservação e posterior quebra de sigilo de registros eletrônicos (logs), observados os requisitos legais, conforme disciplina a lei do Marco Civil da Internet.

A crise de autenticidade exige que a produção da prova digital acompanhe a evolução tecnológica. Além de demonstrar a existência de um conteúdo, é importante comprovar sua integridade e sua origem, garantindo que a evidência seja confiável e apta a sustentar teses processuais e futuras decisões em processos judiciais.

A CRISE DA IDENTIDADE NO SISTEMA FINANCEIRO

Se antes a tecnologia servia para confirmar identidades, hoje ela também permite criá-las, inclusive quando a pessoa por trás da identidade não existe. A IA generativa reduziu drasticamente o custo de criação de identidades sintéticas, acompanhadas de evidências digitais capazes de simular, com elevado grau de verossimilhança, a existência de uma pessoa legítima.

No setor financeiro, isso se traduz em um novo desafio interno: verificar se um cliente realmente existe.

Isso exige a reavaliação de controles que, até pouco tempo atrás, eram considerados suficientes. A biometria, por exemplo, foi concebida para reduzir incertezas sobre a identidade do usuário, mas o avanço dos *deepfakes* e de outras técnicas de manipulação digital tornou a própria prova visual questionável.

Para mitigar riscos, as instituições precisam investir em tecnologias de validação e em camadas adicionais de autenticação. O resultado são processos mais complexos e jornadas mais longas para o usuário, tensionando o equilíbrio entre segurança e experiência do cliente que a própria regulação prudencial e de conduta pressupõe. Encontrar esse ponto de equilíbrio hoje é uma decisão de governança, não de tecnologia, e depende de políticas, controles e treinamentos capazes de evoluir no mesmo ritmo da IA.

DEEPFAKES E FRAUDES DIGITAIS: REFLEXOS TRIBUTÁRIOS DE OPERAÇÕES NÃO AUTORIZADAS

Com o avanço da inteligência artificial, as fraudes digitais ficaram muito mais sofisticadas. Hoje, é possível reproduzir a voz e a imagem de executivos para solicitar pagamentos, aprovar contratações ou autorizar transferências que, à primeira vista, parecem legítimas, agravando a crise de autenticidade dos documentos.

Quando a fraude é identificada, os impactos vão além da perda financeira. A empresa precisa avaliar como registrar contabilmente os valores envolvidos, se a perda poderá ser deduzida na apuração dos tributos sobre o lucro e qual será o tratamento de eventual ressarcimento pelo banco, pela seguradora ou por terceiros.

A situação pode ficar ainda mais complexa quando a fraude envolve a emissão de notas fiscais ou a simulação de uma contratação. Nesses casos, será preciso verificar se houve a apropriação de créditos tributários, se as obrigações acessórias transmitidas precisam ser retificadas e quais providências devem ser adotadas em relação aos documentos fiscais emitidos.

Por isso, além de reforçar os controles para a aprovação de pagamentos e operações sensíveis, é importante que a empresa tenha um procedimento definido para casos suspeitos, envolvendo desde o início as áreas jurídica, financeira, contábil e tributária.

Também é essencial preservar as mensagens, os registros de acesso, os comprovantes e os demais elementos relacionados à operação. Essa documentação será necessária não apenas para buscar a recuperação dos valores, mas também para comprovar a ocorrência da fraude e justificar o tratamento contábil e tributário adotado.

Em tempos de crise de autenticidade, em que até a voz e a imagem de uma pessoa podem ser falsificadas, a adoção de controles preventivos e a preservação adequada das provas passam a ser importantes também sob a perspectiva tributária.

PROTEÇÃO ESTRATÉGICA DA REPUTAÇÃO NA ERA DAS FAKE NEWS

A reputação de uma empresa, antes função do marketing e da assessoria de imprensa, agora impacta diretamente governança, risco e estratégia.

Em uma realidade em que notícias falsas podem ser facilmente criadas em uma ferramenta de IA e viralizar em poucas horas nas redes sociais, o antigo manual de gestão de crises já não funciona.

Para conter os impactos de uma crise com eficiência, é importante implementar duas medidas precisam com antecedência: o monitoramento e o plano de ação.

O monitoramento do que é dito nas redes sociais, analisado juridicamente, pode identificar tendências de crise no seu início e antecipar medidas de contenção imediatas.

Já a existência de um plano de ação projetado com cuidado é capaz de definir árvores de decisões estratégicas, estabelecer fluxos de comunicação e evitar escolhas feitas no calor da emoção, que podem se mostrar equivocadas no futuro.

Para citar apenas um exemplo, excluir uma postagem sem a preservação da prova pode comprometer a possibilidade de ingresso com ação judicial para reparação dos danos causados.

Portanto, se já está é difícil saber o que é verdade ou mentira, agir preventivamente é a melhor forma de proteger a reputação da empresa, dos seus produtos e dos seus executivos.

MAIS DADOS, MAIS CONFIANÇA?

Nos dias de hoje, provar que uma pessoa é quem afirma ser se tornou complexo e necessário. Documentos fotografados, reconhecimento facial e videoconferências, antes tratados como elementos confiáveis de verificação, já convivem com *deepfakes*, ataques de injeção de imagem e identidades sintéticas, ameaças examinadas pela ENISA e contempladas, em diferentes categorias, nas diretrizes mais recentes do NIST.

A reação intuitiva das organizações a esse cenário consiste na ampliação de camadas de verificação da identidade, como mais biometria, mais documentos, mais dados comportamentais, mais cruzamentos externos. Apesar de cada recurso reduzir o risco de fraude, também representa um tratamento de dados pessoais, muitas vezes sensíveis. O tratamento de dados biométricos é, inclusive, um dos temas que integra a Agenda Regulatória 2025–2026 da ANPD, ao lado de IA e de tecnologias emergentes que estão entre as prioridades de fiscalização para 2026–2027.

Sob o argumento de que "é segurança", a desconfiança corre o risco de se transformar em vigilância incremental, em que controles adicionais passam a ser adotados sem que haja uma análise de necessidade, proporcionalidade ou impacto sobre os titulares. Segurança, afinal, não constitui base legal autônoma nem afasta a observância dos princípios e das demais exigências da LGPD.

E é aqui que está **o paradoxo: a resposta à crise de autenticidade pode gerar uma crise maior de privacidade**. Mais dados não produzem necessariamente mais certeza, mas aumentam a superfície de ataque, ampliam o impacto em incidentes e a dependência de tecnologias que também falham, erram e podem ser burladas.

A pergunta, portanto, não deve ser só como detectar o falso, mas qual é o custo, em direitos, de provar o verdadeiro. O nível de verificação deve ser compatível com o risco da transação e com as ameaças que se pretende mitigar. Antes de incorporar uma nova camada, é preciso avaliar sua efetiva contribuição, as alternativas menos invasivas, os prazos de retenção e os mecanismos de contestação de erros.

Reconstruir confiança não significa saber tudo sobre todos, mas utilizar apenas os dados necessários para gerar confiança suficiente em cada contexto.

Fontes:
ENISA Remote Identity Proofing — Attacks & Countermeasures
NIST Special Publication 800-63A-4 — Identity Proofing and Enrollment

O QUE A IA NÃO CONTA SOBRE UMA OBRA

A inteligência artificial generativa desafia a noção de autenticidade também no campo da propriedade intelectual. Textos, imagens, músicas e vídeos podem aparentar originalidade, embora não surjam do zero: são produzidos por modelos treinados com grandes volumes de conteúdo preexistente. A questão jurídica, portanto, não se limita a saber quem deve ser reconhecido como autor do resultado. Em alguns casos, é preciso perguntar quais obras tornaram aquela criação possível, como foram obtidas e sob qual fundamento foram utilizadas.

Isso não significa que todo conteúdo gerado por IA seja uma cópia ou que o treinamento resulte, necessariamente, na reprodução perceptível de obras específicas. Os modelos identificam padrões, e a semelhança estética, isoladamente, não comprova uma infração. O problema está na escala e na opacidade do processo. Em 2025, o Copyright Office norte-americano concluiu que diferentes etapas do desenvolvimento de sistemas generativos podem atingir direitos exclusivos e que a licitude do treinamento depende das obras utilizadas, de sua origem, da finalidade do modelo e dos controles sobre os resultados. Também advertiu que o uso comercial de grandes acervos protegidos para gerar conteúdo concorrente, especialmente quando obtidos por acesso ilícito, pode ultrapassar os limites do fair use (uso justo, princípio norte-americano).

No entanto, isto não é unanimidade. O AI Act europeu, por exemplo, exige que os prestadores de modelos de IA de finalidade geral adotem uma política de cumprimento do direito autoral da União e disponibilizem publicamente um resumo suficientemente pormenorizado dos conteúdos utilizados no treinamento. Para empresas que desenvolvem, contratam ou exploram criações sintéticas, a diligência não deve começar no resultado. É necessário verificar a procedência dos dados, as licenças, os termos do modelo, a intervenção humana e os riscos de similaridade. Em uma crise de autenticidade, a obra não pode ser avaliada só pelo que aparenta ser, mas também pela história criativa e jurídica que permanece escondida por trás dela.

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.

VOCÊ CURTE O SOM DE THE VELVET SUNDOWN?

The Velvet Sundown já é um fenômeno. Com um som que lembra o rock psicodélico dos anos 1970, a banda viralizou nas plataformas de streaming e já conta com milhões de reproduções. O visual charmosamente *vintage* dos quatro integrantes contribuiu para aumentar a curiosidade: quem são eles? Onde vivem? Onde começaram? Vai ter turnê?

Fato é que ninguém sabe quem são essas pessoas e há indícios de que elas simplesmente... não existam.

A autoria do projeto permanece cercada de dúvidas, mas tudo indica que um grupo de músicos, programadores e engenheiros de som se uniu para criar, com IA, as músicas, as imagens de divulgação e até a identidade da banda. Pode ser um experimento musical? Sim, mas The Velvet Sundown virou um experimento sobre confiança.

Aí, você pensa: é justo que um projeto criado por IA dispute nossos ouvidos com criações de artistas humanos? Se a música é boa, importa saber quem a criou? Quem deve receber o dinheiro pelos milhões de *plays*; as bandas que inspiraram o projeto, os programadores que o criaram ou o Suno AI?

Quando já não conseguimos distinguir uma banda real de uma artificial, o que significa autenticidade? Fica a reflexão.

Ouça *Dust on the Wind*, do The Velvet Sundown que, no fechamento desta edição, contava com quase 5 milhões de plays só no Spotify:

Ouça no Spotify

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.

O FUTURO DA FRAUDE SERÁ CADA VEZ MAIS HUMANO.

Um dos recados mais fortes do SXSW 2026 foi a centralidade humana. No universo das fraudes digitais, essa perspectiva se confirma, e o comportamento humano desponta como um dos principais vetores de risco.

A fraude do futuro, que já chegou, explora um humano ainda mais vulnerável, em razão do momento de adaptação que vivemos. Estamos diante de um novo patamar de confiança, atenção, urgência, medo, distração, pertencimento e até solidão.

Ao utilizarmos sistemas de inteligência artificial de forma massiva e pouco intencional, temos deixado o pensamento crítico em segundo plano. Esse cenário se torna ainda mais sensível com o avanço da Emotion AI1, em que amizade, romance, terapia e até orientação espiritual começam a migrar do humano para a máquina.
Se, por um lado, ganhamos uma IA mais empática, por outro, colocamos pessoas com menor capacidade crítica diante de sistemas cujas reações se assemelham cada vez mais às suas.

Para quem trabalha com antifraude, a mensagem é clara: **o futuro da fraude será cada vez mais neurocomportamental, marcado por identidades sintéticas, deepfakes, manipulação emocional automatizada e ataques hiperpersonalizados**. Continua sendo essencial proteger sistemas, mas cuidar das pessoas talvez se torne, a partir de agora, uma das medidas mais relevantes de prevenção a fraudes.

O convite, portanto, é para que **não assistamos passivamente a esse novo cenário, mas retomemos, com intencionalidade e espírito crítico, o controle sobre como decidimos, nos relacionamos e sobre quem ou o quê estamos depositando parcela relevante da nossa confiança**.

Se você, como nós, aprecia o tema, não deixe de seguir **Rana el Kaliouby**, cientista da computação egípcia e uma das principais referências mundiais em IA Centrada no Ser Humano.

Artigo escrito por Ana Rita Bibá Gomes de Almeida

PARA DISTRAIR

FILMES

O SHOW DE TRUMAN
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 Amazon Prime.

SÉRIES

BLACK MIRROR | EP. BE RIGHT BACK
Este é o primeiro episódio da segunda temporada e discute a recriação digital de uma pessoa morta a partir de seus dados. É de arrepiar.

Disponível na Netflix.

LIVROS

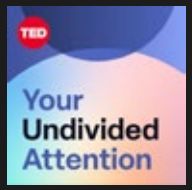
A PRÓXIMA ONDA, DE MUSTAFA SULEYMAN
Lançado em 2023, é um dos livros mais importantes dos últimos anos sobre IA. O autor discute porque tecnologias capazes de criar conteúdo indistinguível do real desafiam governos, empresas e sistemas jurídicos.

Disponível na Amazon

A MORTE DA VERDADE, DE MICHIKO KAKUTANI
A autora, crítica literária do The New York Times por quase quatro décadas e vencedora do Prêmio Pulitzer, analisa como desinformação, relativização dos fatos e manipulação digital corroem a confiança pública. Embora anteceda a explosão da IA generativa, continua extremamente atual.

Disponível na Amazon

PODCASTS



YOUR UNDIVIDED ATTENTION
Um podcast excelente para discutir como a IA, os algoritmos e as plataformas alteram nossa percepção da realidade e da confiança. O episódio **Have We Trained AI to Lie to Itself - and to Us?** conversa diretamente com o tema desta edição.

Ouça o episódio aqui.

O OPICE BLUM NA MÍDIA EM JULHO

Em reportagem publicada pelo Estadão, **Florence Terada**, Sócia Inovação em Serviços Financeiros do Opice Blum, analisa as diferentes abordagens adotadas por Brasil e Noruega no enfrentamento ao vício em apostas esportivas. A matéria destaca as medidas implementadas pelo país europeu para lidar com os impactos da dependência em bets e traz reflexões sobre os desafios relacionados à publicidade, à prevenção e à proteção dos consumidores no ambiente das apostas.

Em artigo publicado pelo Consumidor Moderno, **Camila Jimene**, sócia de Contencioso Digital do Opice Blum, analisa os impactos da decisão do Supremo Tribunal Federal (STF) que estabeleceu novas regras para a responsabilidade das plataformas digitais por conteúdos publicados por terceiros. A análise destaca a ampliação dos deveres atribuídos às plataformas na prevenção, moderação e remoção de conteúdos ilícitos, além dos impactos da decisão para empresas e para o ambiente digital brasileiro.

Em entrevista publicada pelo ClienteSA, **Danielle Serafino**, sócia de LegalX do Opice Blum, participa de debate sobre a maturidade da cultura de experiência do cliente no setor jurídico. A discussão aborda a importância da confiança, da transparência e da construção de relacionamentos mais próximos entre escritórios de advocacia e seus clientes, especialmente diante das transformações provocadas pela tecnologia e pelas novas expectativas do mercado.

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

Ana Rita Biba Gomes de Almeida, advogada de Privacidade, Proteção de Dados e Inteligência Artificial
Anne Pavão Dimantas, advogada de Inovação em Serviços Financeiros
Bruno Blum Fonseca, advogado de propriedade Intelectual, Tecnologia, Mídia e Entretenimento
Camila de Araújo Guimarães, advogada de Privacidade, Proteção de Dados e Inteligência Artificial
Carolina Veludo dos Santos, advogada de Tecnologia, Mídia e Entretenimento
Gabriela Silveira Bueno dos Santos, advogada de Privacidade, Proteção de Dados e Inteligência Artificial
Laura Oliveira Spitzkopf, advogada de Tributário Digital
Mauro Roberto Martins Jr., advogado de LegalX
Pedro Figueiredo Soares, advogado de Inovação em Serviços Financeiros
Rafaella Lowenthal Paulucci, advogada de Tributário Digital
Vinicius Azevedo, advogado de Resposta a Incidentes e Cibersegurança
Juliana Geve, Marketing
Gabriela Dias, Marketing
Nathalia Gomes Silva, Marketing
Sidney Marcos Filho, Designer

Se você gosta da News e quer sugerir um tema para as próximas edições, clique aqui.
Não deixe de compartilhar com alguém que também pode apreciar o conteúdo. Até o mês que vem.