DOSSIÊ DAS BIG TECHS

GOLPES PATROCINADOS

Como as Big Techs transformam fraudes em parte do seu modelo de negócio

SLEEPING GIANTS BRASIL

brief

Especial: Golpes e Fraudes

Golpes e fraudes digitais não são exceções: são engrenagens do modelo de operação das big techs. A dinâmica é simples: primeiro, as plataformas exibem e monetizam anúncios e conteúdos fraudulentos, gerando – e lucrando com – impressões, cliques e conversões. Só depois removem parte deles, quando o dano já ocorreu e a receita já entrou no caixa.

Diante de uma epidemia que atinge dezenas de milhões de brasileiros (1 em cada 3 já foi vítima de um golpe digital) e movimenta bilhões em prejuízos (mais de R$ 111 bi no último ano), as big techs alardeiam que "investem milhões" em prevenção e moderação; mas esses valores são irrisórios frente ao faturamento publicitário. gerado pelas próprias fraudes. Os relatórios de "contas e anúncios removidos" empresas como- Google e Meta não são demonstrações de eficiência, mas sim provas da dimensão industrial do problema: revelam um ecossistema onde campanhas criminosas se infiltram, circulam, convertem e geram lucro para as empresas, antes e apesar de sua intervenção.

Este dossiê reúne argumentos e evidências para uma regulamentação robusta de plataformas e serviços digitais, com dados concretos e referências jornalísticas e acadêmicas que expõem a permissividade das big techs diante do problema. O objetivo é oferecer a cidadãos, formadores de opinião, legisladores e gestores públicos a base factual para enfrentar um sistema que transfere o risco e o prejuízo às famílias e ao Estado, enquanto concentra ganhos bilionários nos caixas das maiores empresas de tecnologia do planeta.

Clique e acesse o site oficial do Dossiê:
https://www.golpespatrocinados.com/

Sumário

1. As plataformas controladas pelas big techs são o principal canal de propagação de golpes digitais. Isso não se deve a uma falha no sistema, mas reflete o modelo de operação das empresas.

As plataformas digitais se tornaram um dos principais vetores de disseminação dos golpes digitais no Brasil e no mundo, não apenas por sua escala e capilaridade, mas sobretudo porque as big techs lucram — e muito — com a circulação de conteúdos fraudulentos. O ponto central não é apenas o quanto essas empresas faturam com as fraudes, mas como faturam: primeiro elas exibem e monetizam anúncios e conteúdos criminosos (impressões, engajamentos, cliques, conversões); e depois — quando o dano já se espalhou — removem uma parte, apresentando os números de bloqueio como prova de eficiência. Essa sequência cria um incentivo perverso: quando uma campanha fraudulenta encontra seu público, gera cliques e converte receita, o sistema publicitário fatura e a intervenção vem a reboque, em ritmo e escala insuficientes para evitar que os prejuízos caiam no colo das vítimas e do Estado.

As big techs se tornaram o vetor dominante dos golpes não só pela capilaridade global, mas porque oferecem exatamente o que o crime precisa para operar em larga escala: alcance massivo, segmentação fina, pagamento integrado, falta de transparência e baixa fricção (fácil usabilidade). A tecnologia criada para servir ao marketing legítimo foi apropriada com facilidade alarmante por golpistas.

Ao contrário de bancos, por exemplo, e de outros setores financeiros que são altamente regulados, sujeitos a deveres claros de diligência, essas plataformas ainda praticam uma autorregulação opaca, priorizando a continuidade da receita publicitária sobre a integridade do ecossistema. Em termos práticos: se o anúncio passa pela moderação automática e começa a rodar, a plataforma cobra, ganha, e só depois do dano é que se discute se o conteúdo se trata de golpe ou não.

Documentos internos da Meta já apontaram que até 70% dos novos anunciantes promoviam golpes, produtos ilegais ou de baixíssima qualidade — um número alarmante, e um sinal de que esse tipo de anúncio é parte relevante do volume de receita da plataforma. Uma segunda leva de documentos internos, obtida pela agência de notícias Reuters, mostrou que a Meta faturou aproximadamente 16 bilhões de dólares em 2024 com a veiculação de anúncios fraudulentos, que promovem golpes e produtos ilegais. Esse valor corresponderia a cerca de 10% da receita anual da companhia.

No Google, há casos de anúncios pagos que aparecem no topo dos resultados de busca, levando a páginas clonadas que capturam senhas, fatores de autenticação dupla e credenciais.

No Google, há casos de anúncios pagos que aparecem no topo dos resultados de busca, levando a páginas clonadas que capturam senhas, fatores de autenticação dupla e credenciais. A empresa recebe por impressões e cliques até que a fraude seja derrubada. Em julho de 2025, a AGU teve de notificar o Google para retirar, em até 24 horas, anúncios pagos que imitavam o site oficial do CNU 2025, usados para cobrança de taxas falsas — ou seja, as peças seguiam rodando quando o órgão interveio.

De tempos em tempos, as empresas donas de plataformas digitais divulgam que bloquearam ou removeram centenas de milhões de anúncios, e suspenderam centenas de milhares de contas devido ao risco de golpes e fraudes. Esses números não provam controle, e sim indicam escala: a existência de um ambiente onde o crime se infiltra continuamente, monetiza as empresas de tecnologia e os golpistas, e só é parcialmente contido.

Há ainda um efeito de leniência por desenho. Registros mostram que contas fraudulentas reincidentes cometem múltiplas infrações e recebem diversas advertências ou “strikes" (8, 16, 32…) antes do banimento. Traduzindo: a plataforma tolera a recorrência do crime enquanto o cliente pagante segue ativo. O banimento vira um mero custo operacional para o fraudador, que abre novas contas com baixíssimo atrito. O resultado é um equilíbrio estável de renda para o crime e para a plataforma: algumas campanhas caem, outras sobem, e a esteira publicitária continua girando. Nessa lógica, a discussão sobre o “quanto” se fatura com fraude perde importância diante do como: a monetização antecede a mitigação, e isso molda comportamentos, prioridades e orçamentos internos.

Enquanto o lucro das big tech vier antes do seu dever de cuidado e proteção dos usuários, o ciclo vai se repetir: golpes entram, geram receita, convertem resultados, e só então parte deles cai — tarde demais para as vítimas, mas no timing perfeito para um modelo que internaliza ganhos e externaliza os prejuízos à sociedade.

2. Os golpes e fraudes digitais são hoje a principal ameaça patrimonial do Brasil – superaram os roubos de rua, e oferecem risco direto ao bolso das famílias e à estabilidade da economia brasileira.

Os golpes digitais se transformaram em um fenômeno de massa, atingindo lares de todas as classes sociais no Brasil. Uma pesquisa Datafolha/Fórum Brasileiro de Segurança Pública revelou que 33,4% da população adulta — cerca de 56 milhões de pessoas — foi vítima de algum golpe financeiro online no último ano. Isso significa que em praticamente todas as famílias brasileiras alguém já foi lesado por uma fraude digital.

As modalidades mais comuns são compras não entregues, PIX e boletos falsos. No primeiro caso, 17,7% da população (quase 30 milhões de pessoas) pagou por produtos ou serviços inexistentes, acumulando perdas estimadas em R$13 bilhões. Já no segundo caso, 14,3% (mais de 24 milhões de pessoas) caíram em armadilhas de transferências falsas, somando prejuízos de R$28,8 bilhões.

Por trás destes números estão aposentados que perderam seu pagamento em um clique, jovens que se endividaram ao tentarem fazer compras aparentemente legítimas e famílias que, ao caírem em golpes, viram sua renda mensal ser corroída. A insegurança digital já impacta o comportamento dos cidadãos: muitos evitam usar meios digitais de pagamento, ou reduzem sua atividade econômica online, por medo das fraudes.

Isso afeta não apenas a confiança das famílias no consumo digital, mas também o tecido social, reforçando a percepção de vulnerabilidade e abandono por parte do Estado.

Enquanto as estatísticas de golpes digitais superam as de furtos e roubos a mão armada, as big techs, que deveriam estar cuidando de nossos espaços digitais, não têm esse cuidado. As plataformas digitais — redes sociais, aplicativos de mensagem, sistemas de anúncios — operam não apenas como vetores de distribuição, mas como infraestrutura de viabilização de golpes em massa, especialmente quando incentivam ou permitem que conteúdos fraudulentos sejam promovidos ou impulsionados, sem que haja filtros robustos de checagem. Isso faz com que as fraudes digitais se propaguem como vírus: as vítimas individuais sofrem perdas diretas, enquanto o Estado e a economia nacional amargam com o esvaziamento de receitas, as restrições de crédito, a insegurança institucional e a redução da confiança no ambiente digital.

3. O crime organizado brasileiro está se transformando – o fuzil agora compartilha espaço com anúncios pagos e contas em aplicativos de mensagens.

Facções criminosas como o Primeiro Comando da Capital (PCC) e o Comando Vermelho (CV), que historicamente disputam rotas de tráfico e territórios, descobriram no espaço digital um campo de expansão mais lucrativo, menos arriscado e com alcance praticamente ilimitado para suas atividades. Hoje, elas lucram bilhões com fraudes digitais, operando como conglomerados criminosos que combinam tecnologia, finanças ilícitas e redes de cooptação. O crime virtual tornou-se peça-chave nas finanças dessas organizações, sendo usado como capital de giro entre outras atividades ilícitas.

O movimento das facções demonstra a consolidação de uma nova tendência nos crimes patrimoniais no Brasil. Os estelionatos eletrônicos cresceram 17% em 2024. No Estado de São Paulo, que concentra grande parte das estatísticas nacionais, os dados são ainda mais eloquentes. Entre 2019 e 2022, os crimes digitais aumentaram 661%, enquanto os estelionatos eletrônicos cresceram 1.162%. Em janeiro de 2019, havia 377 casos registrados; em dezembro de 2022, foram 11.311 em um único mês, um salto de quase 2.900%.

O fato é que o estelionato eletrônico consolidou-se como parte da estratégia central das facções. PCC e CV, no ambiente digital, têm colaborado em operações conjuntas que chegaram a-movimentar R$6 bilhões em fraudes num único ano. No ciberespaço, a rivalidade territorial dá lugar à lógica empresarial: maximizar lucros, explorando falhas de integridade e lacunas de regulação.

Essa escalada vertiginosa não encontra paralelo em nenhuma outra modalidade criminal. Enquanto homicídios, latrocínios e roubos de veículos seguem em queda ou estabilidade, os golpes digitais explodem. É uma tendência que aponta para um deslocamento estrutural: o crime organizado percebeu que, enquanto o assalto à mão armada carrega alto risco de confronto e prisão, o golpe digital garante alto retorno financeiro e baixíssimo risco.

O papel das big techs é central nesse processo. As primeiras investidas das facções criminosas no digital envolveram fraudes de baixa sofisticação, mas de alto volume, como a clonagem de contas de WhatsApp e os famosos “golpes do PIX”, que exploram o popular sistema de pagamentos instantâneos brasileiro utilizando phishing e engenharia social para induzir transferências fraudulentas. Nas redes sociais, as vítimas são atraídas por perfis falsos, e posteriormente são ameaçadas e extorquidas por criminosos. As big techs, ao não estabelecerem filtros eficazes, permitirem a criação de contas falsas e adotarem sistemas de punição lenientes (como permitir dezenas de infrações antes de um banimento), -

tornam-se parte da engrenagem do crime organizado digital.

O resultado é um ciclo perverso: criminosos exploram a confiança das pessoas em plataformas digitais, essas plataformas lucram com a mineração de dados, sem exercer um papel de cuidado eficiente sobre o ecossistema, enquanto as vítimas, famílias e a sociedade brasileira arcam com o prejuízo.

4. Os golpes digitais atingem as pessoas mais vulneráveis, se utilizando de símbolos oficiais e aproveitando momentos de crise extrema para persuadir e explorar.

Os golpes digitais no Brasil não apenas crescem em número absoluto e em sofisticação técnica, como também revelam uma característica perturbadora: eles atingem desproporcionalmente as populações mais vulneráveis. O impacto é devastador: famílias que já vivem em condições de fragilidade financeira, social ou informacional acabam duplamente vitimizadas — primeiro pela crise estrutural, depois pela fraude que instrumentaliza seu desespero.

Em novembro de 2025, o projeto Brief identificou na Biblioteca de Anúncios da Meta 16 mil anúncios ativos que mencionavam a palavra "empréstimo". Desses anúncios, 52% apresentavam indícios de fraude, enquanto 9% eram golpes confirmados. A pesquisa encontrou ofertas de crédito fácil, rápido e sem burocracia, com atendimento "sem consulta ao SPC". A segmentação das plataformas ajuda os golpistas a acessarem o público ideal, as pessoas que necessitam de crédito rápido no Brasil.

Golpes combinando Bolsa Família e o PIX têm disparado no Brasil. Criminosos criam links fraudulentos que prometem valores extras associados ao programa para capturar dados pessoais de beneficiários. Por exemplo: no início de agosto de 2025, circulava em diversas redes sociais um vídeo fraudulento prometendo o Bolsa Família a pessoas que ganham até R$5 mil mensais, com uso de IA e técnicas de persuasão, induzindo usuários a clicar em links falsos e disponibilizarem seus dados pessoais e bancários para os golpistas. A pesquisa do Projeto Brief também identificou anúncios ativos na Meta direcionados a beneficiários do Bolsa Família e do Benefício de Prestação Continuada com links que levam para contas falsas no WhatsApp, e para formulários que capturam dados pessoais, solicitam o pagamento de taxas inexistentes e lucram com a promessa de alívio financeiro.

O alcance desses conteúdos é ainda mais significativo quando eles são monetizados e impulsionados pelas plataformas. Numa ação civil pública movida em março de 2025, a Advocacia-Geral da União (AGU) protocolou uma Ação Civil Pública contra a Meta para obrigar a empresa a coibir anúncios fraudulentos que utilizam símbolos oficiais, imagens de autoridades ou manipulações visuais com o objetivo de aplicar golpes financeiros. Com base em um estudo do NetLab - UFRJ, foram identificados 1.770 anúncios fraudulentos que prometiam supostos valores a receber pela população e distorciam regras de transações via PIX, utilizando símbolos governamentais para dar aparência de legitimidade. A ação da AGU acusa a Meta de ter um sistema de verificação de anúncios ineficiente, em desacordo com seus próprios termos de uso.

Num pedido de ação urgente do STF, a AGU reforçou esse diagnóstico, ao apresentar exemplos extraídos da biblioteca de anúncios da Meta. Tratavam-se de conteúdos fraudulentos prometendo falsas indenizações do INSS, bem como validando medicamentos jamais aprovados pela ANVISA, todos impulsionados com recursos pagos, e se utilizando dos símbolos e logotipos dos órgãos oficiais.

Quadrilhas também estão pagando ao Google para disparar e-mails patrocinados que simulam comunicações dos Correios, conduzindo vítimas a links de phishing (cobrança de taxas inexistentes, atualização de cadastro, etc.) e capturando dados e dinheiro. Em um dos casos, o CNPJ usado pelo anunciante era de uma microempresa que nada tinha a ver com o dos Correios do Brasil — indício de que a verificação de anunciantes falhou. A plataforma, enquanto isso, faturou com as impressões e cliques, antes da eventual remoção dos anúncios.

Casos como esses mostram que os golpes não são apenas uma questão criminal, mas também um problema de integridade institucional. A confiança nos órgãos do Estado é corroída quando logotipos oficiais são apropriados em escala massiva por fraudes veiculadas em plataformas que lucram com sua divulgação.

Outro estudo do NetLab - UFRJ acrescenta mais uma camada a esse problema: a exploração de contextos de crise. Durante as enchentes no Rio Grande do Sul, identificou-se a circulação de anúncios e conteúdos patrocinados que pediam doações fraudulentas, explorando a solidariedade da população em um momento de vulnerabilidade. Essa prática demonstra a rapidez com que criminosos aproveitam catástrofes ou emergências para criar campanhas falsas, impulsionadas nas redes. Mais uma vez, as plataformas receberam para veicular esses anúncios, mas não ofereceram mecanismos ágeis de bloqueio. O resultado foi a dupla vitimização: das famílias que já haviam sido atingidas pela tragédia e foram usadas como isca, e dos cidadãos de outras regiões que, querendo ajudar, tiveram seu dinheiro desviado por golpistas. A lógica de crescimento a qualquer custo das plataformas se mostrou incompatível com o dever de cuidado básico em momentos de calamidade.

5. Enquanto as bigs techs faturam, pessoas públicas e autoridades e são vítimas da exploração de sua credibilidade na aplicação de golpes e fraudes digitais – que chegam a trazer riscos para a saúde pública.

A atual epidemia de golpes e fraudes digitais deve ser potencializada pela inteligência artificial e pelas dinâmicas de desinformação política. Já se observa o uso de deep fakes e vozes clonadas em golpes que imitam familiares pedindo dinheiro, explorando laços afetivos. Essa mesma tecnologia vem sendo usada para criar vídeos falsos de pessoas públicas e autoridades validando produtos e serviços, ampliando exponencialmente o poder de convencimento das fraudes.

Tome-se o exemplo do médico cancerologista e escritor Dr. Drauzio Varella. Foram diversas tentativas – inclusive judiciais – de coibir a veiculação de anúncios fraudulentos com seu nome. Em um artigo publicado em outubro de 2025, o Dr. Drauzio mais uma vez denunciou que quadrilhas vêm cometendo crimes contra a saúde pública se utilizando das redes sociais, usando sua imagem e voz manipulada por IA para vender "remédios" falsos. Ele afirma que plataformas como Instagram e Facebook funcionam, na prática, como parceiras desses golpistas, ao permitir e monetizar esses anúncios até que sejam derrubados. É um alerta de dentro do campo da saúde: golpes pagos e conteúdos enganosos não só drenam dinheiro de pacientes vulneráveis, como corroem a confiança na ciência e nas políticas de saúde, ao vestir fraudes com o verniz de figuras públicas e marcas conhecidas.

O laboratório NetLab da UFRJ mapeou 3.710 anúncios fraudulentos nas plataformas da Meta, entre julho e dezembro de 2024, que usavam indevidamente a imagem e o nome do Dr. Drauzio Varella para vender "tratamentos" sem base científica. As peças violavam diversas normas brasileiras de publicidade brasileiras (publicidade enganosa na área da saúde, uso indevido de imagem) e evidenciam falhas de moderação e verificação da plataforma, já que os anúncios circulavam com segmentação paga, explorando a confiança em figuras científicas e midiáticas para induzir consumidores ao erro. Os autores concluem que a arquitetura publicitária das plataformas facilita um mercado ilegal com impactos na saúde pública e na confiança na ciência.

Esse trabalho se insere em um quadro mais amplo já documentado pelo NetLab: monitoramentos anteriores apontaram milhares de anúncios com deep fakes de celebridades (como William Bonner, Ana Maria Braga e o próprio Dr. Drauzio) promovendo remédios e cosméticos, o que reforça o padrão de apropriação de imagens de alta credibilidade para dar

verniz de legitimidade a promessas falsas. Em síntese, a pesquisa mostra que o problema é sistêmico: anúncios enganosos de saúde não são exceção, mas proliferam em escala por meio da infraestrutura paga de alcance e segmentação das plataformas, que lucram com impressões e cliques antes de eventuais remoções.

O próprio Oversight Board da Meta afirmou, em junho de 2025, que a empresa "provavelmente está permitindo uma quantidade significativa de conteúdo de golpe" nas suas plataformas e que revisores "não estão empoderados" para aplicar, em escala, a proibição de deep fakes e falsas endossos de celebridades usados para fraudes — recomendando, então, que a Meta mude sua abordagem de cumprimento. O caso analisado envolveu um vídeo manipulado de Ronaldo Nazário promovendo um app de aposta, com 600 mil visualizações antes da remoção. A conclusão do Board é que a Meta "não está fazendo o suficiente" para combater esse tipo de golpe.

6. A UE já impõe deveres de diligência e multas significativas às big techs que veiculam campanhas fraudulentas. No Brasil, o STF abriu espaço para a responsabilização. Porém, sem uma regulamentação mais robusta, a epidemia de fraudes digitais seguirá.

A imposição de deveres de diligência e sanções robustas contra fraudes digitais já se tornou realidade na União Europeia. Por meio do seu Digital Services Act (DSA), a UE exige que plataformas de grande porte implementem mecanismos proativos de detecção, mitigação e remoção de conteúdo ilícito, incluindo golpes e fraudes, sob pena de multas que podem alcançar até 6% do faturamento global da empresa. Com base no DSA, a Comissão Europeia enviou requisições formais de informações ao Google, Apple e Microsoft para explicar como essas empresas lidam com anúncios fraudulentos, aplicativos falsos e listagens enganosas em suas plataformas.

Desde março deste ano, a Irlanda lidera uma proposta na UE para obrigar big techs como o Google e a Meta a verificarem previamente anúncios financeiros e a barrarem golpes antes da veiculação. O empurrão regulatório surge após estimativa de €4,3 bilhões em perdas por golpes online na Europa em 2022; e ao menos metade dos países-membros apoia a ideia. O pacote discutido inclui ainda regras de estorno automático às vítimas, e se articula ao DSA, respondendo a críticas de que as plataformas lucram com anúncios enganosos e agem tardiamente. A medida sinaliza uma mudança de ônus: de "remover depois" para "prevenir e-responder com diligência", sob risco de sanções.

Enquanto isso, no Brasil, o regime anterior do artigo 19 do Marco Civil da Internet condicionava a responsabilização das plataformas à existência de ordem judicial específica para remoção de conteúdo de terceiros, mantendo-as em posição de quase impunidade diante da publicidade veiculada em seus espaços. Porém, em 26 de junho de 2025, o STF considerou esse dispositivo parcialmente inconstitucional, afirmando que tal modelo não protege adequadamente direitos fundamentais como dignidade, privacidade e segurança digital. Agora, plataformas poderão responder civilmente quando não removerem conteúdos manifestamente ilícitos — incluindo anúncios pagos ou conteúdos impulsionados — mesmo sem notificação ou ordem judicial anterior.

O fato é que a responsabilização das plataformas ainda aguarda regulamentação legislativa definida. E é previsível que essas empresas mobilizem seus lobbies no Congresso para diluir ou obstruir sua responsabilização, argumentando riscos à liberdade de expressão, insegurança jurídica ou impactos à inovação digital.

Se essa resistência prevalecer e não houver regulação robusta, a epidemia de fraudes e golpes digitais continuará,

alimentada pela conivência institucional e pela continuidade de um modelo de negócios que lucra com a circulação de conteúdos ilícitos.

7. O Brasil precisa agir agora: proteger cidadãos, economia e democracia exige enfrentar as big techs.

As big techs são parte essencial do sistema de propagação de golpes e estelionatos digitais. Elas oferecem a vitrine, cobram pelo espaço e, quando pressionadas, se escoram em políticas internas insuficientes e em respostas lentas para seguir lucrando. Isso porque o negócio da fraude tornou-se parte do modelo de negócio das plataformas. Sem responsabilização firme e sem deveres legais claros de diligência, transparência e prevenção, Google, Meta e outras gigantes continuarão sendo cúmplices e beneficiárias do crime digital, transformando vulnerabilidades sociais em oportunidades de receita, e deixando que famílias, empresas e o próprio Estado arquem com o prejuízo.

O Google já aplica checagem prévia de anunciantes em alguns mercados, sobretudo em serviços financeiros, onde exige certificação antes da veiculação. Porém, trata-se de uma cobertura segmentada, restrita a esse tema. A Meta também possui verificações prévias em certos nichos: exige autorização para anúncios sobre política/temas sociais e pode solicitar verificação/licença para anúncios de produtos financeiros. Por exemplo, no Reino Unido, plataformas como Google, Bing e Meta passaram a barrar promoções financeiras pagas que não sejam aprovadas por firmas autorizadas. A verdade é que existem "ilhas" de verificação prévia nas duas empresas — porém voluntárias, fragmentadas, restritas a algumas geografias, e insuficientes como dever-legal amplo de diligência para cobrirem outras categorias de golpes (p.ex., "Correios" falsos, deep fakes de celebridades vendendo "cura milagrosa").

Se as big techs preveem o risco – porque, ao monetizar anúncios, segmentam públicos e controlam o seu funil de veiculação – devem criar meios técnicos para mitigá-lo e subir seu padrão de diligência para prevenir fraudes. Por exemplo, implementando a verificação reforçada de anunciantes de temas sensíveis (como anúncios de cunho financeiro ou ligados a "benefícios do governo"), fazendo uma remoção ágil após notificação qualificada, tendo mecanismos anti-recidiva (promovendo o bloqueio de contas, domínios e criativos reincidentes), garantindo ampla transparência aos anúncios e conteúdos impulsionados, preservando de provas para investigação, e garantindo que haja transparência de suas taxas de detecção e tempo de resposta.

Por isso, a importância de uma regulação que estenda a verificação, a prevenção e a obrigação de transparência a todo o ecossistema de anúncios, com padrões obrigatórios, auditorias independentes e sanções proporcionais, e não apenas um sistema em que as plataformas decidem, por conta própria, onde vão criar mecanismos de visibilidade e controle.

Somente uma regulamentação firme de serviços digitais que obrigue as big techs à responsabilização pode reverter esse cenário. Enquanto não houver uma norma clara, haverá espaço para lentidão na

atuação preventiva, e exploração de brechas e interpretações que favorecem a impunidade. Sem uma lei que imponha deveres de cuidado, diligência e transparência, e com sanções proporcionais, continuaremos testemunhando uma epidemia de fraudes que lucra com a omissão das big techs — colocando em risco não apenas usuários e consumidores, mas toda a estrutura de confiança no ecossistema digital e na eficiência institucional no nosso país.

Referências

AGÊNCIA PÚBLICA. Remoção de conteúdo está em 40% dos processos contra big techs. Disponível em: https://apublica.org/2025/09/remocao-de-conteudo-esta-em-40-dos-processos-contra-techs/. Acesso em: 3 nov. 2025.

AGU. AGU move ação contra Meta para coibir golpes que usam símbolos de governo e imagens manipuladas nas redes. Disponível em: https://www.gov.br/agu/pt-br/comunicacao/noticias/agu-move-acao-contra-meta-para-coibir-golpes-que-usam-simbolos-de-governo-e-imagens-manipuladas-nas-redes. Acesso em: 3 nov. 2025.

AGU. AGU notifica Google para remoção de anúncios falsos do CPNU 2025. Disponível em: https://www.gov.br/agu/pt-br/comunicacao/noticias/agu-notifica-google-para-remocao-de-anuncios-de-links-falsos-do-cpnu-2025?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

AGU. AGU pede ao STF que adote de imediato medidas contra desinformação e violência digital. Disponível em: https://www.gov.br/agu/pt-br/comunicacao/noticias/agu-pede-ao-stf-que-adote-de-imediato-medidas-contra-desinformacao-e-violencia-digital. Acesso em: 3 nov. 2025.

BRIEF. Fraude, IA e Dinheiro Falso: Como a Meta Lucra Bilhões com Golpes e Exploração de Famílias Carentes no Brasil. Disponível em: https://www.projetobrief.com/quem-paga-a-banda/fraude-ia-e-dinheiro-falso. Acesso em: 6 nov. 2025.

CNN BRASIL. Golpes virtuais financeiros afetaram cerca de 56 milhões de brasileiros. Disponível em: https://www.cnnbrasil.com.br/nacional/brasil/golpes-virtuais-financeiros-afetaram-cerca-de-56-milhoes-de-brasileiros/. Acesso em: 3 nov. 2025.

CONJUR. Fraudes digitais e o STF: um novo capítulo na responsabilidade das plataformas. Disponível em: https://www.conjur.com.br/2025-jun-30/fraudes-digitais-e-o-stf-um-novo-capitulo-na-responsabilidade-das-plataformas/. Acesso em: 3 nov. 2025.

DRAUZIO VARELLA. Estelionatários acobertados. Disponível em: https://drauziovarella.uol.com.br/artigo-do-drauzio-varella/estelionatarios-acobertados/. Acesso em: 3 nov. 2025.

ENGADGET. The Oversight Board says Meta isn't doing enough to fight celeb deepfake scams. Disponível em: https://www.engadget.com/social-media/the-oversight-board-says-meta-isnt-doing-enough-to-fight-celeb-deepfake-scams-194636203.html?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

EUROPEAN COMMISSION. Digital Services Act: Commission sends request for information to Meta on the protection of elections. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373. Acesso em: 3 nov. 2025.

FINANCIAL CONDUCT AUTHORITY (FCA). Reducing and preventing financial crime. Disponível em: https://www.fca.org.uk/publications/corporate-documents/reducing-and-preventing-financial-crime?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

FINANCIAL TIMES. Ireland leads charge to force Big Tech to vet financial ads. Disponível em: https://www.ft.com/content/29dd8525-d837-4abd-abc6-761c3bd78638?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

FOLHA DE S.PAULO. Golpes: 32 milhões foram chantageados por dados vazados. Disponível em: https://www1.folha.uol.com.br/cotidiano/2025/08/brasil-teve-32-milhoes-de-pessoas-chantageadas-por-dados-vazados-em-um-ano-diz-pesquisa.shtml. Acesso em: 3 nov. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. A consolidação de uma nova tendência nos crimes patrimoniais no Brasil. Disponível em: https://fontesegura.forumseguranca.org.br/a-consolidacao-de-uma-nova-tendencia-nos-crimes-patrimoniais-no-brasil/. Acesso em: 3 nov. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. A metamorfose digital: como as facções brasileiras estão trocando o fuzil pelo phishing. Disponível em: https://fontesegura.forumseguranca.org.br/a-metamorfose-digital-como-as-faccoes-brasileiras-estao-trocando-o-fuzil-pelo-phishing/. Acesso em: 3 nov. 2025.

FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Crimes digitais em alta, crimes violentos em queda: um retrato da migração criminal no Estado de São Paulo. Disponível em: https://fontesegura.forumseguranca.org.br/crimes-digitais-em-alta-crimes-violentos-em-queda-um-retrato-da-migracao-criminal-no-estado-de-sao-paulo/. Acesso em: 3 nov. 2025.

G1. Meta faturou US$16 bilhões com anúncios de golpes e produtos ilegais em 2024, diz agência. Disponível em: https://g1.globo.com/tecnologia/noticia/2025/11/06/meta-lucrou-us-16-bilhoes-com-anuncios-de-golpes-e-produtos-ilegais-em-2024-diz-agencia.ghtml. Acesso em 7 nov. 2025.

INFOMONEY. Datafolha: Golpes virtuais atingem 1/3 dos brasileiros e envolvem R$ 112 bi em 1 ano. Disponível em: https://www.infomoney.com.br/brasil/datafolha-golpes-virtuais-atingem-1-3-dos-brasileiros-e-envolvem-r-112-bi-em-1-ano/. Acesso em: 3 nov. 2025.

INFOMONEY. Golpistas pagam ao Google para enviar e-mails fraudulentos em nome dos Correios. Disponível em: https://www.infomoney.com.br/brasil/golpistas-pagam-ao-google-para-enviar-e-mails-fraudulentos-em-nome-dos-correios/?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

INSS. Golpistas estão abordando aposentados e pensionistas com a oferta de agilizar devolução de mensalidade descontada. Disponível em: https://www.gov.br/inss/pt-br/noticias/golpistas-estao-abordando-aposentados-e-pensionistas-com-a-oferta-de-agilizar-devolucao-de-mensalidade-descontada-1. Acesso em: 3 nov. 2025.

JORNAL NACIONAL. Golpistas pagam ao Google pelo disparo de e-mails patrocinados com armadilhas para fraudes. Disponível em: https://globoplay.globo.com/v/13727963/?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

LUPA. A Jornada dos Golpes: Como redes sociais e apps de mensagem são explorados por golpistas e fraudadores. (Relatório em PDF). Disponível em: https://assets.lupa.news/232/23249955.pdf. Acesso em: 3 nov. 2025.

LUPA. É golpe: vídeo que promete Bolsa Família para quem ganha até R$5 mil é falso e usa IA. Disponível em: https://lupa.uol.com.br/jornalismo/2025/08/11/e-golpe-video-que-promete-bolsa-familia-para-quem-ganha-ate-r-5-mil. Acesso em: 3 nov. 2025.

LUPA. Falso SAC, deep fake e marcas são armas em golpes digitais, aponta relatório inédito da Lupa. Disponível em: https://lupa.uol.com.br/jornalismo/2025/06/23/lupa-divulga-relatorio-inedito-sobre-a-nova-era-dos-golpes-digitais. Acesso em: 3 nov. 2025.

NETLAB UFRJ. Atingidos Pelas Redes Sociais: os impactos da indústria da desinformação nos consumidores brasileiros. Disponível em: https://netlab.eco.ufrj.br/post/atingidos-pelas-redes-sociais-os-impactos-da-ind%C3%BAstria-da-desinforma%C3%A7%C3%A3o-nos-consumidores-brasileiro. Acesso em: 3 nov. 2025.

NETLAB UFRJ. Conar conversa com redes sociais para tentar coibir anúncios falsos. Disponível em: https://netlab.eco.ufrj.br/post/conar-conversa-com-redes-sociais-para-tentar-coibir-an%C3%BAncios-falsos?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

NETLAB UFRJ. Danos causados pela publicidade enganosa na Meta. Disponível em: https://netlab.eco.ufrj.br/post/danos-causados-pela-publicidade-enganosa-na-meta. Acesso em: 3 nov. 2025.

NETLAB UFRJ. Enchentes no Rio Grande do Sul: uma análise da desinformação multiplataforma sobre o desastre climático. Disponível em: https://netlab.eco.ufrj.br/post/enchentes-norio-grande-do-sul-uma-an%C3%A1lise-da-desinforma%C3%A7%C3%A3o-multiplataforma-sobre-o-desastre-clim%C3%A1ti. Acesso em: 3 nov. 2025.

NETLAB UFRJ. Golpes, Fraudes e Desinformação na Publicidade Digital Abusiva Contra Mulheres. Disponível em: https://netlab.eco.ufrj.br/post/golpes-fraudes-e-desinformac-a-o-na-publicidade-digital-abusiva-contra-mulheres. Acesso em: 3 nov. 2025.

NETLAB UFRJ. "Dr. Drauzio Varella tem a solução dos seus problemas": mapeando anúncios fraudulentos sobre saúde na Meta. Disponível em: https://netlab.eco.ufrj.br/post/dr-drauzio-varella-tem-a-solu%C3%A7%C3%A3o-dos-seus-problemas-mapeando-an%C3%BAncios-fraudulentos-sobre-sa%C3%BAde-n. Acesso em: 3 nov. 2025.

OBSERVATÓRIO DA IMPRENSA. TJSP defere liminar para remoção de links fraudulentos patrocinados no Google Ads. Disponível em: https://www.observatoriodaimprensa.com.br/digital/tjsp-defere-liminar-para-remocao-de-links-fraudulentos-patrocinados-no-google-ads/?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

OVERSIGHT BOARD. Combat Misleading Deepfake Endorsements By Changing Enforcement Approach. Disponível em: https://www.oversightboard.com/news/combat-misleading-deepfake-endorsements-by-changing-enforcement-approach/?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

SERASA EXPERIAN. Fraudes digitais disparam entre jovens: tentativas de golpe crescem 50% entre pessoas de até 25 anos, revela Serasa Experian. Disponível em: https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/fraudes-digitais-disparam-entre-jovens-tentativas-de-golpe-crescem-50-entre-pessoas-de-ate-25-anos-revela-serasa-experian/. Acesso em: 3 nov. 2025.

TECMUNDO. Brasil: ladrões usando Google Ads para roubar suas senhas e código 2FA. Disponível em: https://www.tecmundo.com.br/seguranca/401571-brasil-ladroes-usando-google-ads-para-roubar-suas-senhas-e-codigo-2fa.htm?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

THE VERGE. The EU is scrutinizing Apple, Google, and Microsoft over online scams. Disponível em: https://www.theverge.com/news/783507/eu-regulators-apple-google-microsoft-online-scams?utm_source=chatgpt.com. Acesso em: 3 nov. 2025.

UOL. Golpes com Bolsa Família e Pix disparam, e governo vê 'epidemia de fraude'. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2025/09/25/golpes-com-bolsa-familia-e-pix-disparam-e-governo-ve-epidemia-de-fraude.htm. Acesso em: 3 nov. 2025.

WALL STREET JOURNAL. Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook. Disponível em: https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8. Acesso em: 3 nov. 2025.

Sobre nós:

SLEEPING GIANTS BRASIL

Movimento de consumidores conscientes, engajados em cobrar comportamentos socialmente responsáveis das marcas. Uma instituição dedicada a defender os interesses dos brasileiros no ambiente digital.

O Sleeping Giants Brasil surgiu em 2020, durante a crise sanitária e informacional da Covid-19, inspirado por uma reportagem que levou três jovens a adaptar no país a metodologia do movimento norte-americano criado em 2016. A iniciativa passou a atuar diretamente na raiz da desinformação — a monetização — conectando consumidores, marcas e plataformas para impedir que receitas financiem conteúdos de ódio e fake news. Desde então, o movimento já retirou cerca de R$ 139 milhões da cadeia de monetização do discurso de ódio. Em quatro anos, consolidou-se como uma instituição sem fins lucrativos reconhecida nacional e internacionalmente, ampliando sua atuação para a defesa dos interesses dos brasileiros e por uma internet mais segura, regulada e democrática.

Site: https://sleepinggiantsbrasil.com/
Instagram: @slpng_giants_pt

brief

O Projeto Brief é uma iniciativa que visa compartilhar inteligência em comunicação para aprimorar narrativas, mapear e antecipar estratégias de comunicação, monitorar investimentos em mídia paga e democratizar o acesso a pesquisas avançadas em comunicação e psicologia social.

O intuito é capacitar atores progressistas para uma comunicação mais assertiva e influente no cenário político atual. Acredita que entender melhor o jogo nos deixa um pouco mais perto de vencê-lo.

Não é preciso se estender muito para constatar a crescente importância da comunicação online na disputa política. Está, para o bem ou para o mal, na nossa cara, no nosso dedão rolando a tela, nas notificações dos grupos de zap, na batalha de hashtags... enfim, em toda parte e influindo cada vez mais nos rumos do país e do mundo.

Site: https://www.projetobrief.com/
Instagram: @projetobrief

Clique e acesse o site oficial do Dossiê:
https://www.golpespatrocinados.com/