Lavanderia do Sucesso: Métricas Digitais Falsas e Crime Penal Econômico

Paulo Moraes

Introdução

A busca pelo *sucesso* nas redes sociais – medido em seguidores, visualizações, curtidas e engajamento tornou-se moeda de troca valiosa na economia digital contemporânea. Entretanto, essa valorização abriu margem para a manipulação fraudulenta dessas métricas, prática que transcende a simples trapaça virtual e ingressa no terreno do **Direito Penal Econômico**. **"Lavanderia do Sucesso"** é aqui concebido como metáfora para esquemas ilícitos que utilizam a falsificação de métricas digitais como meio de alcançar vantagens econômicas indevidas. Este artigo analisa criticamente como a fabricação de popularidade online tem sido instrumentalizada para crimes complexos da lavagem de dinheiro à fraude contra anunciantes, plataformas e investidores – e como a autoridade e influência digitais podem ser artificialmente construídas, gerando efeitos econômicos reais e perniciosos. Abordam-se os possíveis enquadramentos penais dessas condutas no ordenamento jurídico brasileiro (como estelionato, falsidade ideológica, lavagem de capitais e organização criminosa), bem como os desafios de investigação e a relativa omissão estatal diante de delitos digitais sofisticados. Por fim, discute-se o impacto dessas práticas na **legitimidade dos mercados**, no aumento da **desinformação** e na distorção da **livre concorrência**, traçando paralelos com experiências internacionais pertinentes.

Lavagem de Dinheiro por Métricas Digitais Fraudulentas

A **lavagem de dinheiro** tradicionalmente envolve dar aparência lícita a recursos provenientes de crimes. No ambiente digital, surgem esquemas inovadores em que números falsos de engajamento servem a esse propósito. Autoridades financeiras **identificaram estratégias em que organizações criminosas "cooptam" influenciadores ou criam perfis fictícios inflados artificialmente com recursos ilícitos para gerar receitas de publicidade digital (por exemplo, monetização de vídeos ou posts patrocinados)**. Uma vez recebidos pelos indivíduos ou contas envolvidos, esses valores agora com **aparência de ganhos legítimos oriundos de plataformas como YouTube, Instagram ou Facebook** retornam em parte aos cofres do crime organizado, completando o ciclo de branqueamento. Como resumiu um relatório da Unidade de Inteligência Financeira do México, *"é um esquema simples de lavagem: o cartel posiciona o influenciador, a plataforma paga, e o dinheiro já tem aparência de legalidade"*.

Esse método aproveita-se do fato de que **as plataformas digitais não são reguladas com o mesmo rigor dos sistemas financeiros tradicionais**, retardando a detecção de fluxos suspeitos. Somado a isso, a **falta de regulamentação e fiscalização adequada** no setor de mídias sociais facilita a ação de golpistas, permitindo que influenciadores **utilizem suas plataformas para lavar dinheiro proveniente de atividades criminosas e até evadir impostos.** Em outras palavras, criminosos podem camuflar dinheiro sujo *"canalizando verbas por meio de ad exchanges, executando impressões falsas de anúncios em seus próprios sites, e até criando redes de publicidade inteiramente fictícias"*, tornando os recursos aparentemente legítimos. Estima-se que a fraude em publicidade online muitas vezes entrelaçada à lavagem de dinheiro tenha gerado perdas globais em torno de **US$ 100 bilhões apenas em 2023,** valor que ilustra a dimensão econômica avassaladora do problema. Não por acaso, estudos destacam que organizações criminosas, extremistas e mesmo regimes hostis têm se valido desses expedientes tecnológicos não só para lucro,

mas também para financiar atividades ainda mais gravosas, da corrupção à desestabilização de regimes democráticos.

Exemplo marcante ocorreu no México em 2024-2025, quando uma investigação revelou **64 "narco-influenciadores" envolvidos em esquema de lavagem por meio de métricas falsas**. Perfis digitais foram inflados com *bots* e dinheiro ilícito para atrair milhões de seguidores e visualizações, gerando pagamentos de anúncios que, posteriormente, financiavam compra de armas e suborno de autoridades pelo cartel. Sinais reveladores incluíam **a compra maciça de seguidores, interações falsas e até sorteios fraudulentos de prêmios luxuosos** tudo para **dar aparência de legitimidade e sucesso a contas ligadas ao crime.** Em outra frente, a utilização de **personagens digitais falsos** foi detectada: contas em plataformas de conteúdo adulto operadas por *inteligência artificial* geravam receitas milionárias sem nenhuma pessoa real por trás os depósitos vinham de cartões de crédito clonados ou diretamente de recursos do cartel, em mais uma modalidade de lavagem digital de capitais. Esses casos expõem a face insidiosa da *"lavanderia do sucesso"*: números virtuais transformados em dinheiro "limpo", num conluio entre fraude tecnológica e crime organizado.

Fraude contra Anunciantes e o Mercado

Do ponto de vista do **mercado publicitário e dos anunciantes**, a falsificação de métricas configura um esquema de **fraude massiva**. Empresas investem em publicidade ou em parcerias com influenciadores acreditando alcançar um determinado público mas, quando boa parte dos cliques, visualizações ou seguidores são falsos, ocorre **prejuízo financeiro e violação da confiança**. Relatórios internacionais já apontam que a **fraude em anúncios online é hoje uma das modalidades de estelionato mais lucrativas do mundo, superando inclusive golpes tradicionais com cartões de crédito.** Em 2023, **22% de todo o gasto mundial em publicidade digital pode ter sido direcionado a interações falsas** geradas por *bots*, totalizando perdas estimadas em **US$ 84 bilhões** naquele ano.

Esse tipo de fraude assume formas diversas. Uma delas é a **geração automatizada de impressões e cliques em anúncios**, conhecida como *ad fraud*. Redes criminosas constroem websites e aplicativos-fantasma, nos quais inserem anúncios reais; então, por meio de *botnets* (redes de computadores automatizados), simulam milhões de visualizações e cliques nesses anúncios. Os anunciantes pagam acreditando terem alcançado usuários, quando na verdade foram vítimas de uma simulação elaborada. No famoso caso *"Methbot"* (2014-2016), um grupo rentabilizou mais de **US$ 7 milhões em poucos anos enganando milhares de empresas**: eles programaram **servidores para fingirem ser internautas de verdade, carregando anúncios em páginas em branco e até imitando movimentos de mouse, cliques e logins em redes sociais**, tudo para driblar detecções de fraude. O mentor do esquema foi condenado nos Estados Unidos por fraude eletrônica e *money laundering*, recebendo 10 anos de prisão – um indicativo de que tais práticas podem ser combatidas sob as mesmas normas penais do estelionato tradicional em jurisdições que conseguem alcançá-las.

No contexto brasileiro, embora **não haja tipificação penal específica para a fraude de métricas digitais**, estas condutas podem se enquadrar no estelionato do Art. 171 do Código Penal. Basta considerar que o influenciador ou veículo digital que **"inflaciona" seu alcance de modo enganoso, induzindo empresas a contratá-lo ou veicular anúncios a um público inflado artificialmente, obtém vantagem econômica indevida mediante**

ardil, preenchendo os requisitos do tipo penal clássico. Doutrina e jurisprudência pátrias começam a reconhecer essa realidade: ainda que a *compra de seguidores* ou curtidas não esteja expressamente prevista em lei, **os tribunais têm concedido tutela contra tais práticas com base na violação da boa-fé objetiva e do direito do consumidor, entendendo-as como forma de propaganda enganosa**. A advogada Antilia Reis observa, por exemplo, que **usar engajamento falso para promover produtos ou serviços pode ferir o Código de Defesa do Consumidor**, induzindo o público a erro sobre a relevância real daquele influenciador ou marca. Nessa linha, decisões judiciais desde 2022 têm **proibido a compra de seguidores**, reconhecendo o caráter ilícito da manipulação de métricas em prol de vantagens comerciais. Vale lembrar que o CDC brasileiro tipifica como crime fazer publicidade enganosa (art. 67, Lei 8.078/90), cabendo perfeitamente a analogia de que ostentar números falsos para atrair anunciantes é uma forma de anúncio enganoso sobre si próprio.

A fraude contra anunciantes afeta também a **livre concorrência no mercado publicitário e de influenciadores**. Aqueles que se recusam a inflar métricas são prejudicados frente a concorrentes desleais que, munidos de milhões de seguidores fantasmas, capturam contratos e patrocínios indevidos. Trata-se de **distorção do mercado** por meio de meio fraudulento, conduta que guarda semelhança com o conceito de *concorrência desleal*. O direito brasileiro prevê como crime de concorrência desleal, por exemplo, **"empregar meio fraudulento para desviar, em proveito próprio, clientela de outrem"** (art. 195, III, Lei 9.279/96). **Ao falsear seu alcance, um influenciador ou empresa atrai clientela (patrocinadores, público consumidor) alheia de maneira ardilosa**, o que pode perfeitamente ser visto como um desvio de clientela por meios ilícitos. Assim, além do **rombo financeiro** imediato calculado em bilhões a falsificação de métricas corrói a confiança no mercado digital e premia quem frauda em detrimento dos participantes honestos, gerando um círculo vicioso de descrédito.

Fraude contra Plataformas e Investidores

A manipulação de métricas também serve para fraudar as próprias **plataformas digitais e investidores financeiros**. Plataformas como redes sociais e serviços de streaming geralmente remuneram criadores de conteúdo com base em visualizações e engajamento; se esses números são inflados artificialmente, os operadores do esquema estão basicamente **desviando valores indevidos das plataformas**, num equivalente a fraudar uma repartição empresarial. O YouTube, por exemplo, paga uma parcela da receita de anúncios conforme o número de visualizações de vídeos. Um canal que utiliza *bots* para gerar milhões de *views* fantasmas pode receber pagamentos significativos sem ter de fato entregado publicidade a pessoas reais – o que se enquadra como **fraude contra a plataforma e seus anunciantes simultaneamente**. As próprias políticas dessas empresas proíbem terminantemente tais práticas, e quando identificadas resultam em banimento e ações cíveis. Todavia, **quando a fraude atinge montantes elevados ou é praticada de forma organizada, ingressa-se também na esfera penal**. Há casos internacionais em que os responsáveis foram processados criminalmente por enganar plataformas: no esquema *Methbot* já citado, além dos anunciantes enganados, **as plataformas e redes de anúncios também foram vítimas**, pagando a intermediários por tráfego inexistente. O condenado Aleksandr Zhukov e comparsas chegaram a criar uma falsa empresa de publicidade (*Media Methane*) e até leiloar impressões falsas em exchanges de anúncios, ludibriando outras redes e sites parceiros. Em essência, montou-

se um **negócio fictício estruturado para fraudar o ecossistema digital**, o que rendeu acusações de conspiração criminosa e lavagem de dinheiro além da fraude eletrônica em si.

No que tange aos **investidores**, a falsificação de métricas pode configurar fraude societária ou contra o mercado de capitais. Empresas *startups* de tecnologia e redes sociais frequentemente são avaliadas (e financiadas) com base em números de usuários ativos, tráfego e engajamento. Há, portanto, um forte **incentivo perverso** para fundadores ou gestores inflarem esses indicadores a fim de atrair aportes financeiros ou valorizações em bolsa. Tal conduta pode violar diretamente deveres legais de informação verídica a investidores. No Brasil, a Lei 6.385/76 (mercado de valores mobiliários) prevê crime para quem **"induz investidores em erro, por meio de afirmação falsa sobre operação ou situação de empresa"** (art. 27-C), tipificação que abarcaria a divulgação de métricas digitais falsificadas em prospectos, relatórios ou comunicados oficiais. No âmbito penal geral, não há dúvida de que **apresentar dados manipulados de desempenho a um investidor, levando-o a aportar capital de forma equivocada, configura estelionato** ou mesmo crime contra a economia popular (se for o caso de pirâmides ou esquemas de "crescimento" fictício). Por exemplo, se uma rede social informa aos seus acionistas e ao mercado que possui *X* milhões de usuários ativos, quando na realidade parte significativa são contas-robô compradas para inflar os números, administrações podem incorrer em responsabilidade criminal e civil por fraude corporativa.

Um paralelo prático ocorreu com a empresa **Devumi**, nos EUA, não exatamente uma startup buscando investimento, mas uma fornecedora de seguidores falsos que iludiu tanto clientes quanto o mercado. Em 2019, a Promotoria de Nova York celebrou um acordo pioneiro contra essa companhia, que **lucrou cerca de US$ 15 milhões vendendo "curtidas" e seguidores automatizados em redes como Twitter e YouTube**. Além de violar direitos de imagem (os *bots* usavam perfis e fotos de pessoas reais sem consentimento), a prática foi considerada *"deceptive and unlawful"* pelas autoridades, pois **enganava o público e anunciantes sobre a popularidade de certos indivíduos, e até os próprios compradores que achavam estar pagando por engajamento autêntico.** Nesse caso, embora a esfera fosse mais de aplicação de leis de publicidade e defesa do consumidor, fica claro que **a construção artificial de métricas pode também lesar investidores indiretos** – por exemplo, marcas que "investem" em influenciadores inflados ou fundos que patrocinam personalidades digitais sob falsos pressupostos. Em síntese, do ponto de vista penal econômico, **forjar indicadores de performance equivale a falsear demonstrações financeiras**: ambos constituem fraude sobre dados essenciais que orientam decisões de aporte de recursos.

Construção Artificial de Autoridade e Influência

Um dos aspectos mais insidiosos da falsificação de métricas é a **construção artificial de autoridade e influência digital**, com consequências econômicas e sociais tangíveis. Na sociedade da informação, **números são sinônimo de credibilidade**: perfis com milhões de seguidores ou vídeos com visualizações astronômicas tendem a gozar de **maior confiança e notoriedade**, atraindo oportunidades profissionais, comerciais e até políticas. Cientes disso, indivíduos e grupos inescrupulosos utilizam *bots*, fazendas de cliques e outros artifícios para **simular relevância midiática**, em um processo análogo a inflar um currículo com títulos falsos. Essa "autoridade" de fachada pode então ser monetizada ou usada como instrumento de poder. Por exemplo, **um suposto especialista**

com grande audiência (ainda que inflada) pode vender cursos, aconselhar investimentos ou promover produtos financeiros, induzindo seguidores – reais – a lhe confiar dinheiro. Se tais seguidores são enganados a acreditar na competência/alcance do influenciador por causa dos números falseados, há claramente um **dolo em obter vantagem econômica mediante fraude**, mais uma vez alinhando-se aos contornos do estelionato clássico.

O efeito econômico real dessa influência forjada pode ser significativo. Há registros de **golpes financeiros lastreados na autoridade digital**: indivíduos que, turbinados por seguidores fantasmas, promoveram desde esquemas de pirâmide a *"dicas quentes"* de investimentos, causando prejuízos coletivos. Em outros casos, a mera capacidade de **direcionar a opinião de massas** (mesmo que parte seja exército de *bots*) pode ser explorada para manipular mercados – por exemplo, inflar artificialmente a demanda por um ativo ou descredenciar a reputação de concorrentes (*shilling*). Aqui, percebe-se interseção com crimes contra o mercado financeiro e mesmo com **disseminação de desinformação**. Autoridades internacionais já alertaram que **operadores mal-intencionados criam redes inteiras de perfis automatizados para espalhar notícias falsas e promover ideologias extremistas**, aproveitando-se do alcance falso para **desestabilizar setores econômicos e políticos.** Esse tipo de ação, embora muitas vezes tratado na seara eleitoral ou de segurança nacional, possui também um viés penal econômico quando provoca distorções em mercados (p. ex., boatos coordenados afetando ações na bolsa, cambiais ou consumo de certos produtos).

A construção artificial de influência relaciona-se ainda com **a deslegitimação geral dos ambientes informacionais e de negócios online**. Quando o público descobre que *likes* e seguidores podem ser comprados em pacotes (como de fato são **pacotes de 500 mil seguidores ou 5 milhões de visualizações podem ser adquiridos comercialmente**, instala-se a dúvida sobre quem realmente merece prestígio. Essa perda de confiança tem efeito cascata: **marcas passam a duvidar da eficácia do marketing de influência**, investidores se tornam receosos com métricas fornecidas por empresas de tecnologia e mesmo o usuário comum torna-se cético quanto à popularidade de figuras públicas. Em última instância, há uma **erosão da fé pública no valor da "prova social" digital**, o que prejudica não apenas os infratores (quando descobertos), mas todo o ecossistema de creators e negócios legítimos. Economicamente, isso pode se traduzir em retração de investimentos em publicidade digital e em plataformas sociais – afinal, ninguém quer colocar dinheiro em um "jogo marcado por trapaça". Socialmente, a abundância de autoridades falsas gera confusão informativa e dificulta a **livre formação da opinião e do consentimento** do consumidor, bem como **desequilibra a concorrência** pela atenção do público.

Importante salientar que **a conduta de fabricar autoridade digital pode envolver ilícitos penais diversos dependendo dos meios empregados**. Se há *uso de identidade alheia ou criação de personagens inexistentes* (como perfis fictícios com fotos de terceiros), poder-se-á configurar crime de **falsidade ideológica ou falsa identidade**. Especialistas em direito digital no Brasil alertam que criar perfis falsos para obter vantagens pode ser enquadrado como **fraude (estelionato), falsidade ideológica e até difamação**, a depender do contexto. No caso de influenciadores virtuais gerados por IA mencionados anteriormente, que auferiam milhões, houve clara *falsidade* quanto à existência da pessoa – um tipo de fraude ontológica que desafia as categorias jurídicas tradicionais, mas

certamente viola a boa-fé e pode ser tratada como **meio fraudulento de obtenção de ganhos ilícitos**. Assim, a *autoridade fictícia* construída com bits e algoritmos pode dar margem a múltiplos enquadramentos penais, além de representar desafio conceitual novo para o Direito Penal Econômico.

Enquadramentos Penais e Lacunas no Direito Brasileiro

Diante dos cenários expostos, impõe-se identificar quais delitos do ordenamento pátrio poderiam ser aplicados às condutas de falsificação de métricas e crimes correlatos:

- **Estelionato (art. 171 do Código Penal)** – Provavelmente o enquadramento central, dado que quase todas as situações envolvem **obtenção de vantagem econômica mediante ardil, induzindo alguém em erro**. Seja enganando um anunciante, a plataforma, investidores ou consumidores finais, a base é fraudulenta. O estelionato clássico prevê pena de 1 a 5 anos, aumentada de 1/3 se for contra entidade pública ou idoso. Importante notar que a Lei 14.155/2021 introduziu uma qualificadora para fraudes eletrônicas (estelionato cometido mediante dispositivo eletrônico, rede ou serviço de informática), elevando a pena para 4 a 8 anos de reclusão. Ou seja, **o ordenamento já reconhece a maior lesividade das fraudes digitais** equiparando-as em gravidade a crimes como roubo, o que certamente abarcaria golpes envolvendo métricas falsas. Há inclusive projeto de lei buscando tipificar explicitamente o *"estelionato digital"*, com pena de 4 a 8 anos, exemplificado pelo caso *InstaMoney* – golpe que prometia pagamento por curtidas no Instagram e lesou milhares de usuários incautos. Embora tal PL (2339/2023) ainda não tenha virado lei, sua existência sinaliza a preocupação legislativa em acompanhar as novas modalidades de fraude online.

- **Falsidade Ideológica (art. 299 do CP)** – Consiste em **inserir ou omitir informação falsa em documento público ou particular**, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Aplicar esse tipo à manipulação de métricas pode parecer forçado à primeira vista, pois *números de seguidores* não são exatamente um "documento" nos termos clássicos. Contudo, se considerarmos relatórios de alcance, certificados de desempenho ou mesmo prints de tela apresentados em contratos, propostas comerciais ou prospectos de investimento, poderíamos sim ter **documentos ideologicamente falsos** (quando se declara um alcance que se sabe artificial). Ademais, a jurisprudência brasileira já equiparou certas inserções de dados falsos em sistemas informatizados ao crime do art. 299 por analogia. Assim, **apresentar deliberadamente métricas falsas em meios formais** (por exemplo, um *media kit* de influenciador entregue a um cliente, recheado de seguidores comprados como se reais fossem) pode caracterizar falsidade ideológica, concorrendo em concurso material com o estelionato eventualmente. Vale lembrar que a mera criação de perfil falso em rede social, sem uso de nome alheio, não configura crime por si só; porém, caso envolva assumir identidade de terceiro (ex.: perfis fake se passando por pessoa existente), pode incidir o delito de **falsa identidade (art. 307 do CP).** Em suma, no contexto de métricas, a falsidade ideológica seria aplicável quando a fraude ultrapassa o âmbito fático e ingressa no documental ou declaratório, dando suporte escrito à mentira para fins econômicos.

- **Lavagem de Dinheiro (Lei 9.613/1998)** – Conforme discutido, a manipulação de métricas é ferramenta para lavagem quando utilizada para **ocultar ou dissimular a origem ilícita de recursos**. Pelo sistema brasileiro, a lavagem é crime autônomo, acessório a um delito antecedente (tráfico, corrupção, estelionato etc.) cujos proventos se tenta branquear. Nos exemplos trazidos, os crimes antecedentes variam: tráficos diversos no caso dos *narco-influencers* mexicanos, fraudes financeiras no caso de golpistas da internet, ou até pirâmides (crime contra economia popular) nos casos de esquemas tipo InstaMoney. Para configurar lavagem, é preciso a intenção de *"limpar"* o dinheiro ilícito, e no **ambiente digital isso ocorre via múltiplas transações que simulam atividades comerciais legítimas** – como pagamentos de anúncios, doações a influenciadores, assinaturas, compra de bens virtuais, etc. No Brasil, a lavagem de dinheiro é punida com 3 a 10 anos de reclusão (podendo ser aumentada se cometida de forma reiterada ou por organização criminosa). Há um movimento internacional para que crimes cibernéticos lucrativos passem a figurar expressamente como antecedentes da lavagem; de todo modo, nosso ordenamento já permite enquadrar, por exemplo, os ganhos de um golpe online como produto de crime a ser lavado. **Um influenciador que mistura em sua conta bancária doações de fãs honestos com dinheiro originado de fraude** (digamos, por meio de *laranjas* que compram seus produtos com dinheiro ilícito) pode responder por lavagem ao tentar dar licitude a essa mescla. Na prática, como visto, muitas vezes a lavagem via métricas é **orquestrada por organizações criminosas complexas**, requerendo cooperação internacional para sua persecução.

- **Organização Criminosa (Lei 12.850/2013)** – Quando quatro ou mais pessoas se associam de forma estruturada e permanente para cometer crimes cujas penas máximas excedem 4 anos, configura-se a *organização criminosa*. Diversos casos mencionados sugerem a presença desse elemento: quadrilhas especializadas em fraude digital, **empresas de fachada que vendem seguidores falsos**, cartéis empregando equipes de TI para lavar dinheiro via redes, etc. Nesses contextos, além dos crimes-fim (fraude, lavagem), cabe imputar o delito autônomo de participação em organização criminosa, com pena base de 3 a 8 anos. A vantagem de reconhecer a figura da organização é possibilitar técnicas especiais de investigação (interceptações, infiltrações) e punições mais severas aos líderes. Por exemplo, no caso *Methbot*, a complexidade da operação, servidores em diversos países, aluguel de 765 mil endereços IP, falsificação de registros de internet, evidencia uma estrutura profissional e altamente coordenada, análoga a uma organização criminosa transnacional voltada à fraude cibernética. No Brasil, já houve operações policiais, como a **Operação 404** e outras, mirando grupos por trás de golpes digitais, nas quais indiciamentos por associação ou organização criminosa são acrescentados ao rol de crimes, dada a divisão de tarefas entre programadores, recrutadores de *laranjas*, lavadores, etc. No universo de influenciadores, se existir conluio estável por exemplo, **uma "central de bots" que atende diversos criadores de conteúdo fraudulentos**, ou influenciadores que se associam para práticas ilegais (rifas fraudulentas, divulgação de investimentos fictícios) também é possível a incidência dessa lei, como sugerem investigações recentes sobre quadrilhas de apostas ilegais promovidas online.**Outros Enquadramentos** – A depender dos contornos específicos, poderíamos citar

ainda: **Crime contra a Ordem Econômica e Relações de Consumo**, se caracterizada pirâmide financeira (Lei 1.521/51, art. 2º, IX); **Infrações da Lei de Propriedade Industrial (concorrência desleal)**, já mencionadas, quando há desvio de clientela por meios fraudulentos; **Violação de Direitos Autorais ou de Imagem**, quando *bots* usam fotografias e identidades reais sem autorização para criar perfis (art. 184 CP combinado com legislação civil de imagem); e mesmo **crimes contra a fé pública**, se forem utilizados selos, certificados ou elementos de autenticação falsos (por exemplo, *verificado* comprado illicitamente, embora a venda de selos de verificação seja principalmente violação contratual com a plataforma). Convém salientar que, **na prática forense brasileira, os tipos penais clássicos têm sido manejados para cobrir a conduta**, mesmo antes de reformas legislativas específicas. Todavia, **lacunas normativas** ainda existem: não há crime específico para uso de *bots* ou *deepfakes* para fins de fraude, nem tipificação explícita para manipulação algorítmica de relevância (um tema emergente). Essa defasagem legal dificulta a punição direta de certas condutas, obrigando autoridades a buscarem tipos penais genéricos para enquadrá-las.

Desafios de Investigação e Omissão Estatal

A reação do Estado a esses delitos digitais de alto potencial ofensivo enfrenta **consideráveis obstáculos práticos e jurídicos**. Um primeiro desafio é **tecnológico e operacional**: a velocidade e sofisticação com que os golpes ocorrem na internet contrasta com os meios tradicionais de investigação. Delegados especializados apontam que **a obtenção de informações junto às empresas de internet não acompanha a "velocidade da própria internet"**, havendo demora para rastrear IPs e identificar responsáveis. Muitas vezes, os dados necessários (logs de acesso, registros de transações) estão em servidores no exterior, sob controle de corporações que exigem ordens judiciais via cooperação internacional. Mesmo com o **Marco Civil da Internet** (Lei 12.965/2014) garantindo a guarda de registros, o seu art. 10 impõe sigilo e necessidade de ordem judicial para entrega de dados, o que **entorpece investigações urgentes.** Além disso, conforme relato da Polícia Federal, **provedores estrangeiros nem sempre atendem prontamente pedidos das autoridades brasileiras**, e alguns **não possuem representação local**, tornando a persecução um processo lento e burocrático. Enquanto isso, os criminosos se valem de redes privativas, VPNs, criptografia e identidades falsas para se ocultar. A **distância geográfica entre vítima e autor** – frequente em crimes online e a possibilidade de atuação transnacional dificultam a atribuição de responsabilidade e a coleta de provas.

Outro entrave é **estrutural e de prioridade**. Durante anos, delitos como estelionato informático foram vistos como de menor potencial, ou "sem sangue", recebendo atenção inferior em comparação a crimes violentos. **Corpos policiais carecem de efetivo e treinamento especializado**: no Brasil, apenas alguns estados contam com delegacias de crimes cibernéticos bem aparelhadas, e mesmo a PF já registrou que o volume de casos cresce exponencialmente sem que o número de agentes acompanhe. Em 2015, informava-se que a PF contava com grupos dedicados a crimes cibernéticos em somente 15 unidades no país Apesar de avanços desde então (como a criação de unidades especializadas em cada estado e parcerias com órgãos internacionais), **a defasagem de recursos humanos e tecnológicos persiste**. Hackers e fraudadores digitais frequentemente estão um passo à frente, empregando técnicas de mascaramento e evitando deixar rastros facilmente

detectáveis. A **complexidade técnica das perícias** também é alta – por exemplo, analisar bancos de dados de seguidores para distinguir *bots* de pessoas reais requer ferramentas de data science e expertise em redes sociais, nem sempre disponíveis aos peritos oficiais.

Há também certa **omissão ou demora legislativa** em enfrentar especificamente essas novas tipologias criminosas. Enquanto países como os EUA adaptam o uso de leis existentes (como *wire fraud* e *identity theft*) para punir esses casos, e órgãos reguladores usam normas de comércio para coibir a venda de falsos engajamentos, no Brasil temos caminhado mais lentamente. A tipificação de *estelionato digital* ainda tramita, a lei de proteção de dados (LGPD) tangencia apenas parte do problema, e iniciativas voltadas a *fake news* e bots maliciosos (Projeto de Lei das Fake News) encontram resistência e debate acalorado sobre limites à liberdade de expressão. Essa lacuna regulatória deixa **zonas cinzentas** exploradas pelos infratores. Por exemplo, **comprar seguidores ou curtidas não é crime em si**, a não ser que se prove a obtenção de vantagem indevida correlata – o que dificulta punir fornecedores dessa "matéria-prima" da fraude. Somente via Direito do Consumidor ou ações civis tem-se conseguido até agora algum controle, como no caso citado em que a Justiça reconheceu a ilicitude da venda de seguidores falsos e determinou cessação da prática. Especialistas clamam por atualização legal: *"Enquanto pessoas e empresas como a Devumi continuam faturando ao mentir para o público, nós (autoridades) precisamos deixar claro que quem lucra com enganação e falsidade será responsabilizado"*, disse a Procuradora-Geral de NY, Letitia James. Essa mensagem ecoa no cenário brasileiro – a necessidade de **reafirmar que a fraude digital em larga escala não ficará impune**. Contudo, até que as leis se aperfeiçoem e haja investimento pesado em investigação cibernética, **a percepção de impunidade permanece**, incentivando a proliferação desses crimes sofisticados.

Por fim, cabe mencionar a **dificuldade probatória**: diferente de um crime físico onde se apreende o produto ilícito ou se identifica claramente o ato criminoso, nas fraudes de métricas tudo é intangível e pode ser apagado com um comando. A **volatilidade das provas digitais** exige rapidez na atuação do Estado para requisitar dados antes que sejam destruídos. A cooperação das plataformas é crucial – e nem sempre espontânea, pois *likes* e seguidores falsos muitas vezes inflavam também artificialmente os números de tráfego dessas próprias plataformas, que lucram com a atividade intensa. Há, portanto, um potencial **conflito de interesses** ou ao menos falta de incentivo para redes sociais denunciarem ou coibirem agressivamente todos os falsos engajamentos, se isso significar reduzir seus usuários ativos ou visitas. Essa realidade exige regulamentação (impondo deveres de transparência e diligência às empresas de tecnologia) e uma postura mais proativa do Estado. Sem isso, investigações seguirão ocorrendo **a posteriori**, quando o dano já está consumado e os operadores, possivelmente, fora de alcance.

Impactos sobre Mercados, Desinformação e Livre Concorrência

As implicações das fraudes de métricas digitais extrapolam a esfera penal e acarretam **graves distorções econômicas e sociais**. No âmbito de mercados, a onipresença de dados falseados gera um fenômeno de **deslegitimação**. Tomemos o **mercado de publicidade digital e de influenciadores**: se mais de 20% das interações podem ser fictícias, os anunciantes perdem a referência de custo-benefício real e podem retrair seus investimentos, prejudicando inclusive os veículos idôneos. Executivos já descrevem a publicidade online como possivelmente *"a mãe de todas as lavanderias de dinheiro"*, dado o volume colossal de fraude inserido no sistema. Essa reputação abala a

confiança dos investidores no setor de mídia digital e pode demandar custos extras de compliance, auditoria e seguridade, encarecendo a operação para todos. Uma publicação britânica salientou que **a lavagem de dinheiro via anúncios "corrói a confiança na indústria, distorce as dinâmicas de mercado e ameaça os alicerces da publicidade digital"**, afetando a reputação de todo o ecossistema. Ou seja, não se trata apenas do prejuízo financeiro direto, mas também de um **custo invisível em credibilidade e eficiência de mercado**.

No que concerne à **livre concorrência**, conforme já abordado, os agentes que recorrem a fraude conquistam vantagem indevida. Isso caracteriza **competitividade abusiva**: ao invés de competir por qualidade de conteúdo, preço justo ou inovação, compete-se por quem engana melhor os algoritmos e os usuários. Tal prática é antitética ao princípio da livre iniciativa honesta e **viola a isonomia entre concorrentes**. Se deixada sem controle, pode desencorajar novos entrantes (que temem precisar fraudar para sobreviver) e **punir empreendedores éticos com irrelevância** em comparação aos desleais. Em termos jurídicos, é a própria definição de *concorrência desleal*, combatida em diversas legislações. Mesmo no direito antitruste poderíamos vislumbrar implicações: imagine-se uma plataforma dominante que infle seus números de uso para afastar concorrência ou para justificar poder de mercado, haveria impactos concorrenciais e possivelmente configuração de práticas enganosas vedadas.

Outra consequência séria é a **disseminação de desinformação**. Quando números podem ser comprados, **a métrica perde seu valor de indicador de relevância ou veracidade**. Isso abre espaço para que conteúdos de baixa qualidade ou mesmo notícias falsas alcancem destaque imerecido graças a *bots* e perfis fictícios amplificando mensagens. Há um efeito cascata: pessoas reais tendem a confiar ou pelo menos prestar atenção naquilo que parece popular (falácia *bandwagon*). Logo, um agente malicioso pode, mediante investimento financeiro em *fábricas de curtidas*, **fabricar consenso ou trending topics artificiais**, dando impressão de que certa ideia ou produto é amplamente aceito. Esse fenômeno abala processos democráticos (quando usado para fins políticos) e **distorce o comportamento do consumidor**, que é levado a consumir ou investir baseado em modismos fraudulentos. Uma investigação brasileira recente mostrou **perfis falsos usando imagem de celebridades para espalhar golpes de apostas e notícias falsas**, alguns inclusive portando o selo azul de verificação, enganando milhares de seguidores. Isso evidencia como a falsificação de autoridade digital anda de mãos dadas com a **propagação de informações enganosas**, minando a confiança pública na mídia social como fonte de informação.

Por fim, cabe destacar o **dano à ordem econômica e social em sentido amplo**. Mercados funcionam adequadamente quando há **transparência e simetria de informações**. A partir do momento em que métricas elemento-chave de informação na era digital se tornam fundamentalmente não confiáveis, essa simetria se quebra. Temos então um cenário de *"mercado adverso"*: os bons agentes são expulsos ou sufocados pelos ruins (teoria do *market for lemons*). Se cada audiência declarada por um influenciador ou cada estatística de uma startup precisar ser tomada *cum grano salis*, o custo de verificação recai sobre investidores e consumidores, tornando transações menos eficientes. Em última análise, todos pagam esse preço: produtos podem encarecer (para compensar orçamentos de marketing desperdiçados com bots), a inovação pode ser prejudicada

(investimentos canalizados a projetos inflados artificialmente em detrimento de outros meritórios), e a própria **verdade factual** perde valor no discurso econômico.

Perspectivas e Direito Comparado

Ao comparar a situação brasileira com outras jurisdições, nota-se que **o desafio das métricas falsas é global**, mas as respostas regulatórias variam. Nos **Estados Unidos**, como visto, autoridades têm aplicado uma combinação de leis de fraude, lavagem, furto de identidade e normas de publicidade para atacar o problema. Além do caso Zhukov (*Methbot*), em que o perpetrador foi condenado por fraude eletrônica e lavagem, houve ações civis e penais contra diversos esquemas de *click fraud*. A Comissão Federal de Comércio (FTC) americana, por exemplo, **moveu ações contra a venda de indicadores falsos de engajamento,** no caso Devumi, resultando em acordo de US$ 2,5 milhões e proibição da atividade. Promotores estaduais invocaram legislações de proteção ao consumidor e até de *impersonation* (quando perfis falsos envolviam roubo de identidade). Em suma, a tendência nos EUA tem sido enquadrar a venda e uso de métricas falsas como **prática comercial enganosa e fraude eletrônica**, punível tanto civilmente (multas, indenizações) quanto, em casos mais graves, criminalmente.

Na **União Europeia**, ainda que não exista um crime específico unificado de "falsificação de métricas", o tema é tangenciado por várias frentes. O **Regulamento Geral de Proteção de Dados (GDPR)** pode ser acionado se *bots* utilizarem dados pessoais indevidamente, por exemplo. Em nível de consumo, a UE dispõe da **Diretiva contra Práticas Comerciais Desleais**, que proíbe publicidade enganosa, o que poderia abranger influenciadores inflando métricas para ludibriar consumidores sobre sua popularidade ou sobre a qualidade de produtos (imaginando um cenário em que reviews/likes falsos induzem compra). Alguns países têm iniciativas curiosas: na **França**, discutiu-se que astroturfing (campanhas de falso apoio popular online) pode ser enquadrado em fraude. Na **Espanha**, grandes fraudes digitais estão sendo perseguidas sob delitos de estafa e falsedad documental, dependendo dos atos. Observa-se também uma preocupação legislativa crescente em **responsabilizar as plataformas**: o **Digital Services Act (DSA)** da UE, que entrou em vigor em 2023, exige que plataformas adotem medidas para combater bots maliciosos e a manipulação inautêntica de serviços, sob pena de multas severas. Embora focado em conteúdo ilegal e desinformação, indiretamente o DSA pressiona empresas a deterem redes de contas falsas – o que auxiliaria no combate às métricas fraudulentas também.

No **Brasil**, como reiterado, ainda engatinhamos na criação de figuras penais específicas. A jurisprudência pátria começa a punir casos isolados: por exemplo, já houve influenciadores condenados por estelionato ao venderem cursos ou investimentos fraudulentos se valendo de marketing digital agressivo e falso (promessas de retorno garantido com prints de rendimentos forjados, etc.). Contudo, **carecemos de estatísticas consolidadas** sobre perseguição penal de fraudes de engajamento em si. Muitas vítimas (anunciantes lesados, p.ex.) optam por soluções privadas – rescindem contratos, exigem ressarcimento civil – sem acionar a esfera criminal. A depender do porte do prejuízo, isso pode mudar, e a tipificação em andamento de estelionato digital pode facilitar futuras ações penais.

Uma experiência notável vem do **México**, já citada, onde a Unidade de Inteligência Financeira protagoniza esforço interinstitucional contra *narco-influenciadores*. Além de

investigar e bloquear contas, as autoridades mexicanas articulam com o Departamento do Tesouro americano para identificar fluxos ilícitos no sistema financeiro ligados a essas fraudes digitais. Ou seja, o combate está se dando combinando técnicas de **combate à lavagem clássica** (seguindo o dinheiro) com análise de **open source intelligence (OSINT)** nas redes sociais (para detectar anomalias em perfis). Essa abordagem integrada pode servir de modelo a outros países, inclusive ao Brasil: demanda cooperação entre órgãos de persecução penal, reguladores financeiros, empresas de tecnologia e até a sociedade civil (no monitoramento de fake news e bots).

Em resumo, no direito comparado percebe-se uma **tendência de reconhecimento da gravidade do problema e criatividade jurídica para supri-la com as ferramentas existentes**. Países que se destacam no combate a fraudes de métricas o fazem *sem aguardar* a lei perfeita: aplicam-se teorias de fraude, estelionato, lavagem, falsificação, concorrência desleal, conforme o caso, para não deixar esses atos impunes. No Brasil, há margem para seguir o mesmo caminho, usando a analogia e interpretação extensiva **in malam partem** dentro dos limites legais, até que normas mais específicas sejam aprovadas. Ademais, é vital aprender com erros e acertos alheios: a experiência de Nova York no caso Devumi mostrou que, mesmo sem acusação criminal, **uma ação civil robusta e bem divulgada teve efeito pedagógico**, sinalizando ao mercado que comprar seguidores é arriscado e pode render sanções. Da mesma forma, as ações mexicanas sinalizam que **influenciadores associados ao crime organizado** não estão seguros atrás de telas – serão rastreados, mesmo que tardiamente. Essa mensagem de **accountability** precisa ecoar também em solo brasileiro.

Conclusão

A falsificação de métricas digitais nossos *likes*, seguidores e visualizações de cada dia desponta como uma nova fronteira do **crime penal econômico**. Se, numa visão ingênua, comprar seguidores poderia parecer apenas uma trapaça ética ou questão de marketing, a análise jurídica revela um **tecido complexo de ilicitudes** conectadas a essa prática. **"Lavanderia do Sucesso"** não é apenas uma figura de linguagem: representa uma realidade na qual o *sucesso* em redes sociais é fabricado artificialmente para **lavar dinheiro sujo**, **fraudar empresas e indivíduos** e **construir poderes midiáticos fictícios** que podem lesar a economia real. Os criminosos modernos entenderam que bits e algoritmos podem servir tão bem quanto offshores e *laranjas* na ocultação de recursos e na enganação de vítimas – inovando, assim, no modus operandi e desafiando a resposta estatal.

Por outro lado, o **Direito Penal Econômico brasileiro** encontra-se diante do dilema de evoluir para abarcar esses novos fenômenos sem perder de vista os princípios basilares (legalidade, lesividade, proporcionalidade). Identificar a fronteira entre ilicitude penal e mero ilícito civil/ética digital nem sempre é trivial nesse campo. Este artigo procurou demonstrar que, embora nem tudo de reprovável nas métricas falsas esteja ainda positivado em tipos penais específicos, **é possível (e necessário) enquadrar tais condutas nas categorias delitivas existentes**, como estelionato, falsidade e lavagem, quando presente efetiva lesão a bens jurídicos. A sofisticação dos meios – *bot farms*, IA gerando influenciadores falsos, etc. – não pode servir de salvo-conduto para quem causa milhões em prejuízo ou financia atividades ilícitas disfarçado de *digital influencer*.

No aspecto investigativo e preventivo, o caminho adiante exige **investimento em capacidade técnica** do Estado e parcerias com o setor privado. O combate a fraudes de métricas está intrinsecamente ligado ao combate a fraudes cibernéticas em geral, demandando núcleos especializados, inteligência artificial para detecção de padrões anômalos e cooperação internacional ágil. Regulamentações mais claras, seja via **Código Penal** ou legislação extravagante, também seriam benéficas – tipificando condutas como o uso massivo de *bots* para fraude, ou impondo deveres às plataformas de reportarem atividades suspeitas (similar às obrigações de instituições financeiras em casos de lavagem). Porém, ainda que as leis tardem, a interpretação judicial pode e deve avançar no sentido de **não permitir que a impunidade digital se normalize**. Cada vez mais, juízes e promotores entendem o funcionamento desses esquemas, contando com apoio de peritos para traduzir em termos jurídicos as arquiteturas criminosas online.

Em última análise, proteger a *verdade* dos números na era digital é proteger a lisura dos mercados e a confiança coletiva. A economia contemporânea depende imensamente de sistemas de reputação e avaliação online – da escolha de um restaurante pela nota de usuários, à decisão de investir em uma empresa pelo número de clientes que ela alega ter. Se esses sistemas forem sistematicamente manipulados, **rompe-se o pacto de confiança que sustenta as relações econômicas**. Portanto, a repressão penal das fraudes de métricas não tem apenas caráter punitivo, mas também **funcionalidade sistêmica**: desestimular a sabotagem da informação para que a concorrência permaneça livre e leal, o consumidor adequadamente informado e o jogo do mercado, limpo. É uma missão desafiadora, sem dúvida, mas inadiável. A lavanderia do sucesso não pode ficar impune, sob pena de termos um futuro em que a própria ideia de *sucesso* – e por conseguinte, de mérito e valor – estará irremediavelmente lavada, desbotada de significado.

Fontes e Referências:

- Matheus Felipe, *"Influenciadores e apostas: a falsa promessa de riqueza rápida nas redes sociais"*, **Gazeta do Povo** (01/10/2024) – análise sobre monetização ilícita em redes sociais e uso de plataformas para lavar dinheirogazetadopovo.com.brgazetadopovo.com.br.

- Unidade de Inteligência Financeira do México – investigação de *"narco-influencers"* detalhada em **La Opinión** (23/07/2025), mostrando cooptação de influenciadores para lavagem de dinheiro e perfis inflados artificialmente com recursos do narcotráficolaopinion.comlaopinion.com.

- Paula Moraes, **Agência Câmara Notícias** – *"Comissão aprova pena de 4 a 8 anos para estelionato digital"* (08/11/2023), discutindo o PL 2339/23 e exemplificando fraudes que prometem pagamento por curtidas (golpe *InstaMoney*) camara.leg.br.

- Portal Leo Dias – entrevista *"É crime comprar seguidores? Especialista explica tudo!"* (18/10/2023), com advogada Antilia Reis, esclarecendo a ilegalidade do engajamento falso, sua caracterização como propaganda enganosa e possível enquadramento em estelionato e fraude digitalportalleodias.comportalleodias.com.

- Departamento de Justiça dos EUA (Distr. Leste de NY) – Press Release *"Russian Cybercriminal Sentenced to 10 Years for Digital Ad Fraud Scheme"* (10/11/2021), detalhando o caso *Methbot* de fraude massiva por bots simulando humanos, com

prejuízo de US$ 7 milhões, condenado por fraude eletrônica e lavagemjustice.govjustice.gov.

- Julia Linehan, *“4 steps to tackle money laundering in online advertising”*, **The Media Leader** (15/10/2024) – artigo opinativo destacando a conexão entre fraude em métricas de anúncio e esquemas de lavagem de dinheiro, incluindo estimativas de US$ 100 bi em perdas globais e impactos na confiança da indústriauk.themedialeader.comuk.themedialeader.com.
- Jeffrey S. Edelstein, *“Fake Likes, Followers Yield Real Legal Action”*, **Manatt, Phelps & Phillips** (21/02/2019) – resumo do caso Devumi, primeiro enforcement nos EUA contra venda de seguidores falsos, com detalhes do esquema (US$ 15 milhões em vendas de falsos engajamentos) e fundamentos legais invocados (práticas enganosas, uso indevido de identidade) manatt.commanatt.com.
- FrancesNews, *“Perfis falsos usam imagem de Carlinhos Maia em golpes de apostas”* (28/10/2025) – notícia sobre remoção de contas falsas no Instagram que imitavam influenciadores para golpes, com comentário de especialista sobre tipos penais aplicáveis (fraude, falsidade ideológica)francesnews.com.br.
- CPI dos Crimes Cibernéticos – cobertura da **Agência Câmara** (20/08/2015) mostrando dificuldades em rastrear e punir delitos na internet, falta de agilidade na obtenção de dados e carência de efetivo especializadocamara.leg.brcamara.leg.br.
- Dados de mercado de fraude digital – **FraudBlocker/Juniper Research** indicando volume de perdas com ad fraud (2023) fraudblocker.com. Também **Business of Apps** e outras fontes corroborando escala global do problema.
- *(Outras fontes citadas ao longo do texto estão referenciadas nos trechos indicados.)*