

PARECER TÉCNICO CONJUNTO

INTERNETLAB, ALÁFIA LAB, ARTIGO 19 E CONECTAS DIREITOS HUMANOS

COORDENAÇÃO NÃO É INAUTENTICIDADE: PARÂMETROS TÉCNICOS PARA A ANÁLISE DE MOBILIZAÇÕES DIGITAIS

Introdução e apresentação

A política é, por definição, uma atividade coletiva. Cidadãos se organizam, combinam estratégias, compartilham mensagens, convocam manifestações e procuram convencer outras pessoas de suas posições. Hoje, boa parte dessa mobilização acontece nas plataformas digitais e nos aplicativos de mensagens, que se tornaram espaços fundamentais de participação política e debate público. **A existência de coordenação entre usuários não constitui, portanto, uma anomalia do ambiente digital: é uma expressão do próprio exercício da democracia.**

O ordenamento jurídico brasileiro reconhece essa realidade ao disciplinar a propaganda eleitoral na internet, especialmente por meio da Lei nº 9.504/1997 e da Resolução TSE nº 23.610/2019. Mais recentemente, a Portaria TSE nº 463/2026 estabeleceu obrigações de identificação e enfrentamento de comportamentos coordenados inautênticos, exigindo expressamente que as plataformas distingam essas operações da atuação coordenada legítima. Essa distinção é fundamental: **combater redes de manipulação não pode significar tratar como suspeita a organização de cidadãos que procuram ampliar o alcance de suas ideias.** Mensagens padronizadas, hashtags compartilhadas e convocações para ações simultâneas são práticas comuns de participação política e não demonstram, isoladamente, inautenticidade.

O presente parecer parte dessa premissa para responder a quesitos técnicos sobre a identificação de comportamentos coordenados inautênticos, seus critérios de detecção e os limites das medidas adotadas pelas plataformas digitais. Seu objetivo é contribuir para uma avaliação tecnicamente fundamentada dessas práticas, distinguindo mobilizações legítimas de operações que utilizam mecanismos enganosos ou artificiais para manipular o ambiente informacional. Trata-se de uma distinção indispensável para **proteger a integridade do processo eleitoral sem restringir indevidamente a liberdade de expressão, de associação e de participação política dos cidadãos.**

Quesito 1: Como a literatura especializada e as principais plataformas digitais definem o comportamento coordenado inautêntico (CIB)? Quais são seus elementos caracterizadores?

O conceito de **comportamento coordenado inautêntico** (*Coordinated Inauthentic Behavior* – CIB) foi criado pelo Facebook, atual Meta, por volta de 2018. A expressão soa técnica e objetiva, como se houvesse uma categoria óbvia de comportamento online que cruza uma linha claramente demarcada entre o aceitável e o inaceitável. Mas, o CIB é um conceito artificial, assim como sua linha divisória,

demarcados pela indústria de tecnologia. É preciso questionar em que ponto esse conceito confronta com a liberdade de expressão, de associação orgânica e mobilização popular, que são pressupostos do processo eleitoral. Esse conceito passou a ser usado no debate público, na literatura e nas políticas de outras plataformas e é definido, na formulação atual da Meta, como *"esforços coordenados para manipular o debate público com um objetivo estratégico, nos quais **contas falsas são centrais para a operação**"*.¹ A violação essencial do CIB, segundo essa definição trazida pela empresa, ocorre quando redes operam de forma articulada enganando os utilizadores sobre *quem* está por trás da operação, *de onde* ela é gerida ou *qual* o seu verdadeiro propósito. Nos relatórios trimestrais de ameaças, a empresa acrescenta que, *"em cada caso, as pessoas se coordenam entre si e usam contas falsas para enganar os outros sobre quem são e o que estão fazendo"*. Diz também que a aplicação da política se concentra *"no comportamento, não no conteúdo — não importa quem esteja por trás, o que publiquem ou se são estrangeiros ou domésticos"*.²

O TikTok, por sua vez, caracteriza as operações de influência disfarçadas (Covert Influence Operations – CIO) pela atuação de redes de contas destinadas a enganar usuários ou sistemas e influenciar estrategicamente o debate público. O X (antigo Twitter), por fim, proíbe atividades coordenadas inautênticas destinadas a influenciar artificialmente conversas ou manipular a visibilidade de conteúdos, mas reconhece expressamente a legitimidade da coordenação autêntica entre usuários para manifestar apoio ou oposição a causas.

Assim, sua caracterização depende das práticas utilizadas, não da orientação política ou da veracidade dos conteúdos publicados.

Um dos principais trabalhos analisando e definindo o que constituiria essas práticas vem da Universidade de Oxford. Phill Howard e Samuel Woolley cunharam o termo “Propaganda Computacional” e estabeleceram a referência para caracterização dessas práticas.³ Analisando diversas instâncias onde foi identificada manipulação artificial de opinião pública, os pesquisadores definiram propaganda computacional como “o uso de algoritmos, automação e curadoria humana para distribuir intencionalmente informações enganosas em redes sociais”. O objetivo dessa coordenação em regra envolve fazer parecer que uma pauta ou tema possui um engajamento humano que ela de fato não tem, por isso o uso de automação e contas falsas se torna elemento central. Estudos do Stanford Internet Observatory documentam operações de influência que ocultam seus responsáveis por meio de perfis fictícios e outras formas de dissimulação. Dessa forma, três elementos são fundamentais para a caracterização do comportamento coordenado inautêntico: **(i) inautenticidade, sobretudo pelo uso de contas falsas ou personas fictícias, elemento central na definição da Meta, ou de outros mecanismos de ocultação; (ii) intenção de enganar usuários ou plataformas, usualmente para fazer parecer que temas e conteúdos possuem um alto engajamento de pessoas reais, quando na verdade não o tem; e (iii) coordenação entre várias contas ou ativos, atuando em rede.** A simples coordenação de atividades, portanto, não caracteriza CIB, embora possa ser examinada à luz de outras políticas de integridade.

¹ META. Inauthentic Behavior. Transparency Center: Community Standards. Disponível em: <https://transparency.meta.com/policies/community-standards/inauthentic-behavior/>. Acesso em: 22 out. 2026.

² Idem.

³ Samuel C. Woolley & Philip N. Howard, Working Paper 2017.11, Project on Computational Propaganda. Available at:

<https://ora.ox.ac.uk/objects/uuid:d6157461-ae6d-48ff-a9a9-2d93222a9bfd/files/m8be3ef66dde61927afdc7ad7d166b0f4>

Quesito 2: O uso de mensagens padronizadas, hashtags em horários determinados e convocações para ações coletivas pode, por si só, caracterizar comportamento coordenado inautêntico? O que distingue essas práticas da mobilização política legítima?

Não. A utilização de mensagens padronizadas, hashtags e convocações para ações simultâneas constitui prática comum de mobilização política e **isoladamente não caracteriza comportamento coordenado inautêntico**. A própria Meta reconhece expressamente a legitimidade da coordenação entre usuários, inclusive como fundamento de campanhas de arrecadação e movimentos de base (*grassroots organizations*). O X proíbe *"atividade coordenada inautêntica que influencie artificialmente conversas"*, mas trata como permitida a conduta de *"coordenar-se de forma autêntica com outras pessoas para expressar ideias, pontos de vista, apoio ou oposição a uma causa"*, desde que sem violar as regras.

A distinção fundamental está na autenticidade dos participantes e na ausência de dissimulação. Uma mobilização organizada por atores identificáveis, com participação voluntária de usuários reais, difere de operações que empregam contas falsas, identidades fictícias, automação enganosa ou mecanismos para simular apoio popular inexistente. Nesse sentido, a literatura define o *astroturfing* político como uma campanha coordenada de forma central *"na qual os participantes fingem ser cidadãos comuns agindo de forma independente"*⁴. Os autores apontam que padrões como o compartilhamento recíproco também são comuns em campanhas espontâneas legítimas e **geram falsos positivos quando analisados sozinhos**. O problema reside nas práticas de manipulação artificial, e não na utilização de funcionalidades como hashtags, comentários e compartilhamentos para fins de mobilização. Uma revisão recente da literatura classifica movimentos sociais de base, comunidades de fãs e ativistas como casos de coordenação autêntica e inofensiva e também ressalta que a **autenticidade é uma característica dos participantes, e não de suas ações**: é inautêntico quem se apresenta falsamente para enganar sobre quem é ou o que faz.⁵

A legislação eleitoral brasileira adota critério equivalente. O art. 57-B, § 2º, da Lei nº 9.504/1997 proíbe a veiculação de conteúdo eleitoral por meio de cadastro de usuário *"com a intenção de falsear identidade"*. O § 3º veda o uso de *"ferramentas digitais não disponibilizadas pelo provedor da aplicação de internet, ainda que gratuitas, para alterar o teor ou a repercussão de propaganda eleitoral"*. A Resolução TSE nº 23.610/2019 reproduz essas vedações no art. 28, §§ 2º e 3º. Hashtags, convocações e mensagens padronizadas usadas por pessoas reais, por meio das ferramentas oferecidas pela própria plataforma, não se enquadram em nenhuma dessas hipóteses.

Desse modo, uma mobilização convocada abertamente por atores identificáveis, com participação voluntária de usuários reais, é diferente de operações que usam contas falsas, identidades fictícias, automação não declarada ou compra de engajamento para simular um apoio popular que não existe. Mobilizações para ações coletivas no ambiente digital tem no seu centro o engajamento de usuários reais com aquela pauta, o que difere da característica central de falso engajamento de ações de CIB, se aproximando muito mais de mobilizações de rua. A convocação pública, aliás, torna a coordenação transparente, o oposto da ocultação que caracteriza o CIB.

⁴ SCHOCH, David; KELLER, Franziska B.; STIER, Sebastian; YANG, JungHwan. Coordination patterns reveal online political astroturfing across the world. *Scientific Reports*, v. 12, art. 4572, 2022. DOI: <https://doi.org/10.1038/s41598-022-08404-9>

⁵ MANNOCCI, Lorenzo et al. Detection and characterization of coordinated online behavior: a survey. arXiv, 2024. Disponível em: <https://arxiv.org/abs/2408.01257>. Acesso em: 22 out. 2026.

Quesito 3: Qual é o valor de indicadores como sincronização de publicações, repetição de conteúdos e picos de engajamento na identificação de operações inautênticas? Que evidências adicionais são necessárias?

Sincronização de publicações, repetição de conteúdos e picos de engajamento podem ser indícios úteis para identificar possíveis padrões de coordenação, **mas insuficientes, isoladamente, para demonstrar inautenticidade**. A literatura técnica é clara ao separar coordenação de inautenticidade. Nizzoli et al. lembram que ativistas e iniciativas de base costumam apresentar comportamento “coordenado, mas autêntico”, e concluem que “alta coordenação não implica necessariamente inautenticidade”⁶. Esses comportamentos também ocorrem em mobilizações legítimas, especialmente durante eventos políticos de grande repercussão. Na medida em que as fronteiras entre redes e ruas se tornam mais porosas, é possível dizer que essa sincronização online, quando autêntica, se revela como a faceta online do que seria a organização de manifestações e atos nas ruas. Estudos empíricos mostram que métodos baseados exclusivamente em padrões de interação podem produzir falsos positivos, tornando necessária a comparação com grupos de usuários autênticos. Os autores registram que esses erros aparecem “quando o mundo on-line reage a eventos do mundo real”, como o discurso presidencial do Estado da União, que provocou um surto de atividade coordenada entre parlamentares.⁷

A identificação de CIB exige evidências adicionais, como **uso de contas falsas ou comprometidas, automação enganosa, vínculos entre contas aparentemente independentes e ocultação dos responsáveis pela operação**. A Meta declara que suas investigações consideram os comportamentos e as conexões entre operadores, e não apenas os conteúdos publicados. Portanto, a análise estatística deve ser complementada por investigação contextual e técnica capaz de demonstrar os mecanismos de inautenticidade.

Quesito 4: Como as políticas da Meta, do Google e do X diferenciam comportamento coordenado inautêntico, spam e manipulação artificial de engajamento? Essas categorias são equivalentes?

Primeiro, é importante ressaltar que as empresas entendem que as categorias **não são equivalentes**. A Meta distingue o comportamento coordenado inautêntico (CIB), caracterizado pelo uso central de identidades falsas em operações de influência, de outras práticas inautênticas, como *spam* e manipulação artificial de engajamento, que podem ocorrer sem contas falsas. A empresa prevê medidas de fiscalização distintas para essas categorias. O spam, por sua vez, tem política própria, voltada a conteúdo “concebido para enganar, induzir em erro ou sobrecarregar usuários a fim de aumentar artificialmente a audiência”

O X adota uma política mais ampla de autenticidade, que proíbe manipulação artificial de tendências, engajamento fraudulento e *spam*, inclusive por múltiplas contas. Entretanto, **autoriza expressamente**

⁶ NIZZOLI, Leonardo; TARDELLI, Serena; AVVENUTI, Marco; CRESCI, Stefano; TESCONI, Maurizio. Coordinated behavior on social media in 2019 UK general election. In: INTERNATIONAL AAAI CONFERENCE ON WEB AND SOCIAL MEDIA (ICWSM), 15., 2021. Proceedings [...]. 2021. Disponível em: <https://cdn.aaai.org/ojs/18074/18074-28-21569-1-2-20210521.pdf>. Acesso em: 22 out. 2026.

⁷ VARGAS, Luis; EMAMI, Patrick; TRAYNOR, Patrick. On the detection of disinformation campaign activity with network analysis. In: ACM SIGSAC CONFERENCE ON CLOUD COMPUTING SECURITY WORKSHOP (CCSW), 2020. Proceedings [...]. New York: ACM, 2020. p. 133-146. DOI: <https://doi.org/10.1145/3411495.3421363>.

a coordenação autêntica de usuários para manifestar apoio ou oposição a causas. A coordenação autêntica por meio de hashtags em horário marcado, os chamados “tuitaços”, é prática consolidada no Brasil e foi adotada pela própria Justiça Eleitoral. O TSE convocou instituições e cidadãos a publicar com a hashtag #DemocraciaSempre em 15 de setembro de 2023, das 10h às 12h¹⁰, e promoveu o tuitaço #RolêDasEleições em 2022 para estimular o alistamento de jovens eleitores. A diferença em relação à manipulação está no meio empregado. Em 2019, por exemplo, um levantamento feito com dados do DFRLab apontou que hashtags convocadas para um “*twittaço*” foram impulsionadas por perfis com sinais de automação e por poucos usuários publicando repetidamente, conduta que a política da plataforma já vedava.

O Google, por sua vez, possui regras específicas contra manipulação de resultados de busca, tráfego automatizado e engajamento artificial no YouTube, sem tratar essas práticas necessariamente como CIB. A plataforma considera legítimo o engajamento em que “*a intenção principal do usuário humano é interagir de forma autêntica com o conteúdo*”⁸.

As categorias, portanto, não são equivalentes. O CIB exige coordenação, uso central de identidades falsas e o objetivo de enganar sobre quem está por trás da operação para influenciar o debate público. A identificação de uma irregularidade exige, portanto, a indicação da política específica aplicável e dos elementos que caracterizam sua violação. A existência de coordenação não permite presumir, indistintamente, CIB, spam, manipulação de tendências ou engajamento fraudulento.

Quesito 5: Em que medida os canais do WhatsApp desempenham funções equivalentes às de perfis públicos em redes sociais? Quais características devem ser consideradas na identificação de comportamento coordenado inautêntico nesses ambientes?

Os canais do WhatsApp apresentam **equivalência funcional com perfis públicos de redes sociais**, como Instagram, Facebook e X. Permitem que pessoas e organizações construam audiências de seguidores, publiquem conteúdos, recebam reações e ampliem seu alcance por compartilhamentos. Os canais também podem ser encontrados por mecanismos de busca e recomendação, inclusive com critérios de popularidade e engajamento. A própria Meta os apresenta como ferramentas para criadores, organizações e figuras públicas alcançarem e mobilizarem audiências.

A principal diferença está no formato predominantemente unidirecional da comunicação, sem comentários públicos dos seguidores. Isso não altera sua função como espaço de comunicação pública e mobilização coletiva. **Assim como nos perfis de redes sociais, a publicação de orientações para compartilhar conteúdos, utilizar *hashtags* ou participar de campanhas não constitui, por si só, comportamento inautêntico. Nesse contexto é fundamental o fato de que qualquer ação subsequente depende de atividade autêntica, autônoma e voluntária do usuário.**

Não é possível presumir o controle dos usuários que espontaneamente reproduzem essas mensagens em outras plataformas - até porque isso equivaleria a questionar a própria liberdade de expressão e de ação de cada uma dessas pessoas. Ainda, não se pode presumir que os donos de canais têm controle sobre eventual coordenação inautêntica ou uso malicioso por parte de usuários das mensagens que ali são compartilhadas, na medida em que cada usuário pode (ou não) comportar-se da forma como bem entender. Essas características não alteram a função dos canais como espaço de comunicação pública. Elas tornam a análise de eventual inautenticidade, inclusive, mais viável do que em conversas privadas.

⁸ YOUTUBE. Fake engagement policy. YouTube Help. Disponível em: <https://support.google.com/youtube/answer/3399767>. Acesso em: 22 out. 2026.]

Por isso, aplicam-se aos canais os mesmos critérios usados para perfis públicos. Publicar orientações para compartilhar conteúdo, usar hashtags ou participar de campanhas não constitui, por si só, comportamento inautêntico - da mesma forma que uma convocação para um painel ou ato nas ruas não o seria. Enquadrar algo como CIB exige provas adicionais de ocultação ou de manipulação artificial.

Na identificação de comportamento coordenado inautêntico (CIB) nesses ambientes, devem ser considerados: (i) **autenticidade da titularidade do canal**: verificar se o canal se apresenta com identidade verdadeira ou se o administrador se faz passar por outra pessoa ou entidade. As diretrizes do WhatsApp vedam atividades que “*enganem deliberadamente, se façam passar por outrem ou deturpem intencionalmente*” quem as pratica e exigem que o título do canal reflita seu conteúdo; (ii) **origem identificável do conteúdo**: o conteúdo que circula a partir de um canal identificado revela quem o produziu. Para haver CIB, seria necessário demonstrar que essa origem foi ocultada por outros meios; (iii) **limites técnicos de viralização**: cada mensagem ou atualização de canal só pode ser encaminhada para até cinco conversas por vez; (iv) **distinção entre o canal e a conduta de terceiros**: não se pode presumir que o administrador controle os usuários que, por iniciativa própria, reproduzem as mensagens em outras plataformas. A própria arquitetura do serviço impede o administrador de conhecer a identidade de quem o segue.

Em síntese, os canais do WhatsApp são espaços de comunicação pública equivalentes a perfis em redes sociais e devem ser analisados com os mesmos critérios. A coordenação, a convocação e o alcance elevado não bastam. É preciso demonstrar a inautenticidade e o vínculo do responsável pelo canal com os mecanismos de manipulação.

Quesito 6: Quais são os principais riscos técnicos e para os direitos dos usuários decorrentes da classificação indevida de mobilizações políticas legítimas como comportamento coordenado inautêntico?

A classificação indevida pode produzir falsos positivos, levando à remoção de conteúdos, suspensão de contas, restrição da visibilidade de manifestações políticas legítimas e violação à liberdade de expressão. É o risco de enquadrar como inautêntica uma mobilização que é legítima, que por sua vez tem impacto direto nos direitos de livre associação e manifestação. Esse risco é documentado na literatura. Ao comparar campanhas de desinformação com comunidades legítimas que também se coordenam, Vargas, Emami e Traynor registraram queda expressiva de precisão nos modelos de detecção. Os erros aumentavam justamente quando os usuários reagiam a eventos reais de grande repercussão.⁹

Esses riscos são especialmente relevantes em períodos eleitorais, quando a coordenação entre cidadãos, movimentos sociais e campanhas é parte essencial da participação democrática. A própria Meta reconhece que a organização coletiva constitui fundamento legítimo de movimentos populares e campanhas de mobilização.

Além das restrições diretas, a aplicação excessivamente ampla de políticas contra CIB pode gerar efeitos inibidores sobre a liberdade de expressão e de associação, desestimular a participação política e prejudicar desproporcionalmente determinados grupos. As diretrizes eleitorais da Comissão Europeia, por sua vez, exigem medidas proporcionais, transparentes e que

⁹ VARGAS, Luis; EMAMI, Patrick; TRAYNOR, Patrick. On the detection of disinformation campaign activity with network analysis. In: ACM SIGSAC CONFERENCE ON CLOUD COMPUTING SECURITY WORKSHOP (CCSW), 2020. Proceedings [...]. New York: ACM, 2020. p. 133-146. DOI: <https://doi.org/10.1145/3411495.3421363>.

preservem direitos fundamentais. Pede também que as plataformas demonstrem, durante os períodos eleitorais, que suas decisões de moderação “*não afetam a igualdade entre candidatos nem favorecem ou promovem de forma desproporcional vozes que representem determinadas posições*” (item 32). Por isso, a classificação de uma operação como inautêntica deve ser fundamentada em evidências verificáveis, acompanhada de salvaguardas contra erros e mecanismos de contestação.

Além das restrições diretas, a aplicação excessivamente ampla das políticas contra CIB pode desestimular a participação política e comprometer a liberdade de expressão e de associação. As *Guidelines on the Mitigation of Systemic Risks for Electoral Processes*, da Comissão Europeia, recomendam que as medidas de integridade eleitoral sejam avaliadas quanto à eficácia, às consequências não intencionais e aos impactos sobre direitos fundamentais (itens 28 e 33). Também ressaltam a necessidade de evitar efeitos desproporcionais sobre determinadas posições políticas e a igualdade entre candidatos (item 32). Por isso, medidas restritivas devem estar fundamentadas em evidências verificáveis e acompanhadas de salvaguardas contra erros e mecanismos de contestação.

, particularmente presentes em períodos eleitorais, é útil para demonstrar os riscos de interpretações equivocadas a respeito de mobilizações digitais legítimas. A convocação de uma manifestação, que é voluntário. Restringir a liberdade de que tais manifestações sejam convocadas, pela mera existência de um canal que permite esse tipo de comunicação a um grupo que voluntariamente optou por receber tais comunicados, seria evidentemente uma violação de direitos fundamentais e de certa forma uma afronta ao próprio processo democrático. O mesmo deve ser válido para as manifestações em ambientes digitais. Da mesma forma, a mecânica específica de engajamento de cada um durante uma manifestação de rua também é (e sempre pode ser) distinta, o que faz parte da própria premissa de liberdade neste contexto. Se não fosse assim, qualquer ato individualmente praticado por qualquer pessoa que faz parte de uma manifestação ou a apoia poderia ser atribuído à totalidade das pessoas presentes e, mais, os líderes da manifestação teriam de ser responsabilizados por quaisquer atitudes praticadas pelos manifestantes, independentemente do seu efetivo envolvimento com cada conduta específica.

Se a esfera pública é cada vez mais digital, é evidente que o engajamento dos cidadãos eleitores também ocorrerá cada vez mais dentro desse ambiente, o que implica a necessidade de regulá-lo, mas também de assegurar sua capacidade de promoção de mobilizações legítimas, de divulgação de ideias, e de debate.

Quesito 7: Quais são os principais parâmetros e boas práticas internacionais para identificar e enfrentar comportamentos coordenados inautênticos, preservando a liberdade de expressão e a participação política legítima?

As boas práticas internacionais seguem três eixos: identificação baseada no comportamento e nos meios empregados, proporcionalidade das medidas com proteção dos direitos fundamentais, e garantias processuais para os usuários atingidos. As diretrizes da UNESCO e da Comissão Europeia para a integridade eleitoral exigem que medidas de mitigação de riscos considerem seus possíveis impactos sobre a liberdade de expressão e de associação, o que é o caso diante de falsos positivos na moderação de eventual comportamento inautêntico. Os Princípios de Santa Clara reforçam a importância de critérios transparentes, notificações fundamentadas e mecanismos efetivos de contestação.

Na identificação de CIB, a Meta prioriza o comportamento dos operadores e o uso de contas falsas, independentemente das posições políticas ou do conteúdo divulgado. Investigações do Stanford Internet Observatory também demonstram a importância de examinar redes de perfis fictícios,

dissimulação de identidade e outros mecanismos de engano, enquanto os parâmetros definidos por pesquisadores de Oxford apontam para o uso de automação de forma coordenada para enganar sobre o a identidade de quem publica e o engajamento real da pauta. A coordenação política legítima não deve ser confundida com operações inautênticas, e eventuais medidas restritivas devem ser justificadas por evidências específicas, proporcionais e sujeitas a revisão.

Quesito 8: Considerando o art. 14 da Portaria TSE nº 463/2026 e sua remissão ao art. 9º-D da Resolução TSE nº 23.610/2019, a detecção e a desarticulação de comportamentos inautênticos coordenados pressupõem vínculo demonstrável com a circulação de fatos notoriamente inverídicos ou descontextualizados que atentem contra a integridade do processo eleitoral? Quais elementos caracterizam esse vínculo e distinguem as redes inautênticas da atuação coordenada legítima?

O art. 14 vincula expressamente os mecanismos de detecção e desarticulação de redes inautênticas à finalidade de prevenir ou reduzir a circulação de desinformação que ameace a integridade do processo eleitoral. Sua aplicação pressupõe, portanto, **um nexo material entre os comportamentos investigados e esse risco específico**, não bastando a identificação de atividades coordenadas ou de estratégias coletivas para ampliar o alcance de mensagens.

Esse vínculo deve ser avaliado a partir de evidências de inautenticidade — como identidades falsas, dissimulação ou manipulação artificial — e de sua relação com a circulação efetiva ou com riscos concretamente identificados de desinformação sobre o processo eleitoral. A detecção preventiva não exige comprovação prévia de um ilícito, mas medidas restritivas demandam fundamentação proporcional à sua gravidade. A própria Resolução TSE nº 23.610/2019 protege expressamente o compartilhamento simultâneo de conteúdos e a utilização coordenada de hashtags por apoiadores.

Quesito 9: Caracterizada a hipótese, quais providências podem ser adotadas pelas plataformas, por iniciativa própria, e quais podem ser determinadas pela Presidência do TSE? Esclarecer os respectivos fundamentos, limites e requisitos, distinguindo a supervisão administrativa dos planos de conformidade das medidas que dependam de decisão jurisdicional, especialmente quanto à limitação de alcance, interrupção da atuação de redes, suspensão de contas e remoção de conteúdos, observadas a proporcionalidade, a reversibilidade e as garantias de contestação.

A regulamentação distingue **medidas de iniciativa própria dos provedores, poderes de supervisão administrativa e medidas jurisdicionais**. As plataformas podem adotar ações preventivas e corretivas, incluindo ajustes nos sistemas de recomendação, restrições graduadas à atuação de redes inautênticas e interrupção da circulação ou monetização de conteúdos ilícitos, observadas as hipóteses legais e suas políticas de integridade. O art. 14 exige que essas medidas sejam proporcionais, temporárias quando cabível, reversíveis e acompanhadas de mecanismos de contestação. A exclusão de perfis por iniciativa do provedor recebe tratamento específico no art. 38-A, § 2º, que a restringe às hipóteses de perfis falsos, automatizados ou robôs.

À Presidência do TSE, **no exercício da supervisão administrativa dos planos de conformidade**, compete requisitar informações, exigir adequações, determinar auditorias e adotar as providências de acompanhamento previstas na Portaria nº 463/2026. Essa competência não se confunde com autorização genérica para determinar a remoção de conteúdos, a suspensão de contas ou a interrupção de canais legítimos. Tais medidas, quando impostas pela autoridade pública, dependem de competência e fundamento jurisdicionais próprios. A Resolução nº 23.610/2019 exige fundamentação

específica, mínima interferência no debate democrático, delimitação do conteúdo atingido e garantias processuais, inclusive contraditório e ampla defesa nas hipóteses de remoção de perfis previstas no art. 38-A.

A eficácia das medidas de integridade deve considerar seus efeitos sobre a igualdade de tratamento entre candidatos, o pluralismo e a participação política, inclusive os riscos de restrições desproporcionais decorrentes de classificações equivocadas.

REFERÊNCIAS

- Comissão Europeia. [Guidelines on Electoral Risks under the DSA](#). 2024.
- Google. [Perguntas frequentes sobre o Google Trends](#).
- Google. [Spam Policies for Google Search](#).
- InternetLab. [Campanha eleitoral no Facebook: Bolsonaro, Haddad e Lula nas eleições de 2018](#). 2018.
- InternetLab. [Comportamento inautêntico no Instagram](#). 2022.
- InternetLab. [Compromisso com a democracia: integridade eleitoral e plataformas](#). 2023.
- InternetLab. [Iguais perante as plataformas?](#) 2023.
- Meta. [Inauthentic Behavior Policy Update](#). 2019.
- Meta. [Removing Additional Inauthentic Activity](#). 2018.
- Meta. [Removing Coordinated Inauthentic Behavior](#). 2020.
- Meta. [WhatsApp Channels Are Going Global](#). 2023.
- Santa Clara Principles. [Transparency and Accountability in Content Moderation](#).
- Stanford Internet Observatory. [Political Retweet Rings and Compromised Accounts](#). 2020.
- Stanford Internet Observatory e Graphika. [Unheard Voice](#). 2022.
- UNESCO. [Guidelines for the Governance of Digital Platforms](#). 2023.
- USC. [Investigating State-Backed Information Operations](#). 2025.
- WhatsApp. [About Creating a Channel](#).
- WhatsApp. [Channels Privacy Policy](#).
- WhatsApp. [How WhatsApp Recommends Channels](#).
- X. [Authenticity Policy](#). 2025.
- X. [Como usar hashtags](#).
- X. [Trends Recommendations](#).
- YouTube. [Política contra engajamento falso](#).