

**GUIA
INTERNET,
DEMOCRACIA
E ELEIÇÕES**

VOLUME II

cgib.r



Esta obra foi publicada nos termos da licença
Creative Commons, Atribuição 4.0 Internacional.
creativecommons.org/licenses/by/4.0/deed.pt_BR

egi.br

GUIA
Internet,
Democracia
e Eleições
volume II

setembro de 2026

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR

DIRETOR-PRESIDENTE: Demi Getschko

DIRETOR DE APOIO ÀS ATIVIDADES DO CGI.BR:

Hartmut Richard Glaser

DIRETOR DE SERVIÇOS E TECNOLOGIA: Frederico Neves

DIRETOR DE PROJETOS ESPECIAIS E DE DESENVOLVIMENTO:

Milton Kaoru Kashiwakura

DIRETOR ADMINISTRATIVO E FINANCEIRO: Ricardo Narchi

CRÉDITOS DA PUBLICAÇÃO

COORDENAÇÃO EDITORIAL:

Comitê Gestor da Internet no Brasil – CGI.br

PESQUISA E REDAÇÃO DO RELATÓRIO: Clarissa Mendes (Assessora Técnica de Políticas Públicas Digitais do CGI.br), Juliano Cappi (Gerente de Políticas Públicas Digitais do CGI.br)

REVISÃO: Nathália Corvello (Redatora Técnica do CGI.br) e Clarissa Mendes (Assessora Técnica de Políticas Públicas Digitais do CGI.br)

ILUSTRAÇÕES E PROJETO GRÁFICO: Dânica Machado

DIAGRAMAÇÃO: Dânica Machado

COMITÊ GESTOR DA INTERNET – CGI.br

REPRESENTANTES DO SETOR GOVERNAMENTAL: Alexandre Freire, Cláudio Furtado, Cristiane Rauen, Débora Peres Menezes, Hermano Barros Tercius, José Roberto de Moraes Rêgo Jr., Luanna Roncaratti, Pedro Helena Pontual Machado e Renata Mielli

REPRESENTANTES DO SETOR EMPRESARIAL: Cristiano Flôres, Henrique Faulhaber, Marcos Ferrari e Nivaldo Cleto

REPRESENTANTES DO TERCEIRO SETOR: Bia Barbosa, Bianca Kremer, Percival Henriques e Rodolfo Avelino

REPRESENTANTES DA COMUNIDADE CIENTÍFICA E TECNOLÓGICA: Lisandro Zambenedetti, Marcelo Fornazin e Rafael de Almeida Evangelista

REPRESENTANTE DE NOTÓRIO SABER EM ASSUNTO DE INTERNET:

Demi Getschko

COORDENADORA: Renata Mielli

SECRETÁRIO-EXECUTIVO: Hartmut Richard Glaser

DADOS INTERNACIONAIS DE CATALOGAÇÃO NA PUBLICAÇÃO (CIP)

Guia Internet, democracia e eleições [livro eletrônico] : volume II / [editor] Núcleo de Informação e Coordenação do Ponto BR. -- São Paulo : Comitê Gestor da Internet no Brasil, 2026.

PDF

Bibliografia.

ISBN 978-65-6165-050-2

1. Eleições – Brasil 2. Internet nas campanhas eleitorais – Brasil 3. Propaganda política 4. Notícias falsas 5. Desinformação 6. Inteligência Artificial 7. Fontes de referência – guias e manuais

I. Núcleo de Informação e Coordenação do Ponto BR.

CDD-302.23

Índices para catálogo sistemático:

1. Internet : Meios de comunicação : Aspectos sociais

Lucas Meirelles Rangel Rodrigues - Bibliotecário - CRB-8/9701

302.23

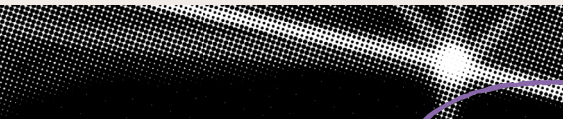
PRINCÍPIOS DO CGI.BR PARA REGULAÇÃO DE PLATAFORMAS DE REDES SOCIAIS¹

O Comitê Gestor da Internet no Brasil (CGI.br), a partir de seu modelo multissetorial, que congrega representantes da sociedade e do governo, adotou por consenso uma série de princípios para a construção de um marco regulatório sobre plataformas de redes sociais. Esses princípios promovem um ambiente digital mais seguro e transparente, além de terem sido fundamentais na construção deste Guia.



ESTADO DEMOCRÁTICO DE DIREITO, SOBERANIA E JURISDIÇÃO NACIONAL

As atividades das plataformas de rede social devem respeitar a supremacia da Constituição Federal e o ordenamento jurídico do país, garantindo a prevalência e a jurisdição do Estado brasileiro de aplicar suas leis, medidas e políticas para a proteção do Estado Democrático de Direito, da democracia, da segurança e direitos de seus cidadãos. As plataformas também devem promover a diversidade das expressões culturais do território em que atuam e o desenvolvimento socioeconômico do país.



2

DIREITOS HUMANOS, LIBERDADE DE EXPRESSÃO E PRIVACIDADE

Os direitos humanos são interdependentes e não hierarquizáveis. A regulação deve assegurar a proteção da dignidade humana e dos direitos fundamentais, incluindo a liberdade de expressão, consideradas suas dimensões individual e coletiva, a privacidade, a igualdade, o direito à não discriminação e a proteção absoluta aos direitos da criança e do adolescente, buscando combater a incitação à violência, ao discurso de ódio e a todas as formas de discriminação nas redes sociais.

3

AUTODETERMINAÇÃO INFORMACIONAL

A regulação deve promover meios que permitam aos usuários decidir informadamente quando, como e em que medida seus dados pessoais podem ser coletados, usados, armazenados e compartilhados. Especialmente em tratamento de dados não essenciais, como processos de perfilização, moderação e recomendação de conteúdos, a autodeterminação informacional deve ser exercida sem prejuízo no acesso ao serviço. Inclui também o direito de usuários e grupos escolherem a que informações querem ter acesso, como o padrão da oferta de conteúdos que lhes é destinada com base em seus dados pessoais.

4

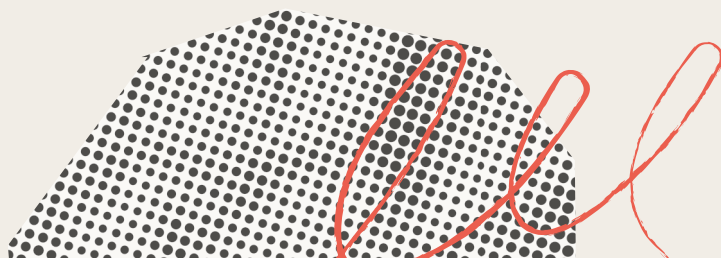
INTEGRIDADE DA INFORMAÇÃO

A regulação deve atuar para proteger o direito à informação e promover a precisão, consistência e confiabilidade dos conteúdos, dos processos e dos sistemas de informações. Para a manutenção de um ecossistema informacional íntegro, saudável e seguro, devem ser promovidas informações de interesse público, como conteúdos jornalísticos e científicos, e desenvolvidas medidas de enfrentamento a fraudes e à desinformação. Deve promover, também, a garantia da preservação da memória, determinando a criação de mecanismos para organizar e armazenar conteúdos — mesmo que não disponíveis ao público — para fins de pesquisa e registro histórico.

5

INOVAÇÃO E DESENVOLVIMENTO SOCIOECONÔMICO

A regulação deve estimular a inovação, a autonomia tecnológica e o desenvolvimento socioeconômico, criando condições para a geração de renda, a valorização de produtos e serviços, o surgimento de novas formas de trabalho (respeitados os parâmetros de trabalho decente²) e o fortalecimento da economia digital promovendo o ambiente competitivo e plural. Deve-se incentivar a diversidade de modelos e a viabilidade econômica de iniciativas baseadas na colaboração e no bem comum e contribuir para uma economia digital mais inclusiva e sustentável.



6

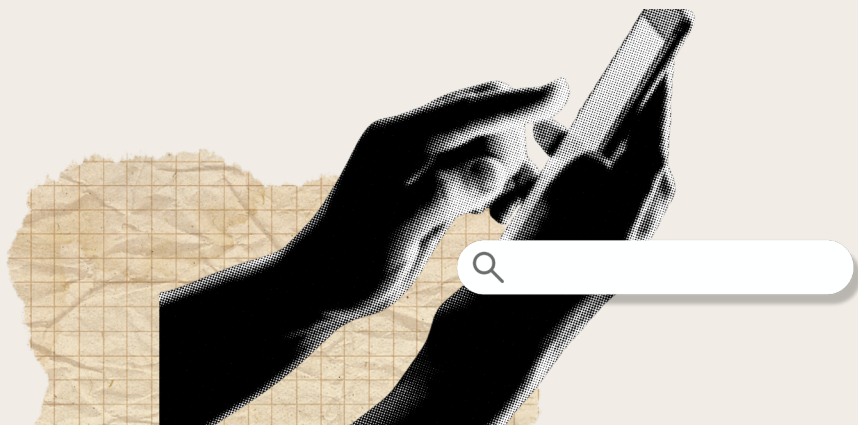
TRANSPARÊNCIA E PRESTAÇÃO DE CONTAS

As plataformas de redes sociais devem ser transparentes e prestar contas com relação ao seu funcionamento, inclusive sobre os mecanismos de impulsionamento, distribuição, moderação e recomendação algorítmica e sobre políticas de monetização. Devem ser proporcionados meios adequados de verificação das remoções de conteúdos, garantindo o devido processo. As plataformas devem oferecer aberturas qualificadas de dados relevantes para pesquisadores independentes e autoridades públicas.

7

INTEROPERABILIDADE E PORTABILIDADE

A regulação deve garantir aos usuários de redes sociais o direito de portabilidade, permitindo a transferência de dados em um formato estruturado, comumente usado e legível por máquina. Deve também promover a interoperabilidade, isto é, a capacidade de diferentes serviços digitais se comunicarem em tempo real, permitindo que usuários combinem serviços com funcionalidades similares, ressalvados os desafios técnicos, jurídicos e de segurança. Nesse contexto, deve ser promovido o emprego de protocolos e padrões abertos.



8

PREVENÇÃO E RESPONSABILIDADE

As plataformas de redes sociais devem adotar medidas preventivas eficazes de mitigação para reduzir os riscos sistêmicos decorrentes do desenho, funcionamento e diretrizes de seus serviços, sobretudo aqueles que possam favorecer a disseminação de conteúdos lesivos ao Estado Democrático de Direito e aos direitos fundamentais. Quando tais riscos resultarem em danos, incumbe-lhes a responsabilidade pela devida reparação.

9

PROPORCIONALIDADE REGULATÓRIA

A regulação deve reconhecer a pluralidade e o dinamismo de atores no ecossistema digital, prevendo obrigações de acordo com as diferenças de porte, de atividades e de impacto das plataformas de redes sociais, adotando modelos assimétricos e proporcionais que considerem essa diversidade e mecanismos de revisão periódica de critérios.

10

AMBIENTE REGULATÓRIO E GOVERNANÇA MULTISSETORIAL

A regulação das redes sociais deve estruturar-se a partir de um arranjo institucional robusto, composto por órgãos da administração pública dotados das capacidades necessárias ao exercício eficaz de suas competências, e incluir instituições e entidades independentes. Este modelo deve ser orientado por uma governança multissetorial, que reconheça e corrija as assimetrias de participação entre os distintos atores garantindo o interesse público.

ÍNDICE

- ↗ **12** Apresentação
- ↗ **16** Internet e plataformas digitais
- ↗ **24** Eleições, democracia e Internet: o desafio da IA generativa
 - 28** I. O uso de *deepfakes* em contexto eleitoral
 - 30** As *deepfakes* impactam ou não impactam nas decisões eleitorais?
 - 33** Violência política de gênero e *deepfakes*
 - 36** II. O uso de *chatbots* como fonte de informações eleitorais
- ↗ **38** Como combater desinformação nas eleições
- ↗ **46** E eu, o que posso fazer?
- ↗ **54** Saiba mais

APRESENTAÇÃO



Ao longo de décadas, a Internet consolidou-se como infraestrutura essencial para a sociedade contemporânea e para o exercício de direitos fundamentais, tornando-se parte das atividades do nosso dia a dia para buscar, receber e difundir informações^{3 4}, utilizar serviços de governo, fazer compras e muito mais.

Desde a década de 2010, a Internet foi gradativamente ultrapassando a televisão e se convertendo no principal ambiente de acesso à informação para a maior parte da população mundial^{5 6}. Dentro da dinâmica das redes, os padrões também mudaram. Em 2026, pela primeira vez, as mídias

sociais e as redes de vídeo se tornaram a principal forma de acesso a notícias *online* no mundo, superando as fontes de notícias tradicionais⁷.

No Brasil, é por intermédio das **plataformas digitais** que os brasileiros acessam informações sobre o que está acontecendo no mundo, no país ou na cidade. No último ano, o principal meio através do qual os usuários de Internet relataram receber, ver ou procurar informações diariamente foram aplicativos de mensagens (60%), seguidos por *feeds* de vídeos curtos (53%), *sites* ou aplicativos de vídeos (50%) e *feeds* de notícias em redes sociais (46%)⁸.

Esse uso impõe vários desafios, uma vez que, de um lado, o **acesso** universal e significativo à Internet ainda não é a realidade para uma parcela importante da população⁹ e, de outro, as plataformas que intermedeiam os fluxos comunicacionais são empresas privadas orientadas por objetivos econômicos, e não pela perspectiva do interesse público.

Desde 2018, o CGI.br tem empregado esforços para o enfrentamento da disseminação de desinformação, que ganhou contornos de uma verdadeira indústria e se tornou um dos problemas públicos centrais no país e no mundo, estabelecendo novos desafios para a garantia do processo democrático. Quando o primeiro *Guia Internet, Democracia e Eleições*¹⁰ foi publicado pelo CGI.br em 2018, alguns dos desafios que enfrentamos hoje já se faziam presentes, despertando preocupações sobre o papel que a Internet pode exercer nas eleições.

Entre março e abril daquele ano, o caso da Cambridge Analytica expôs a estratégia de coleta e tratamento de informações de mais de 50 milhões de pessoas sem consentimento empregada pela empresa¹¹. O objetivo era a realização de propaganda política microdirecionada a favor de Donald Trump nas eleições estadunidenses, ocorridas em 2016.

Os processos eleitorais realizados nos Estados Unidos e Reino Unido em 2016 representaram um marco. Os consensos até então estabelecidos sobre o papel das tecnologias na política eleitoral foram desafiados pelo reconhecimento amplo da função desempenhada por um conjunto de fenômenos, como anúncios direcionados, câmaras de eco, *bots*, entre outros, no resultado de eleições¹². Isso contribuiu para que a palavra “pós-verdade” fosse escolhida como a palavra do ano pelo Oxford Dictionary¹³.

Naquele contexto, como explorado pelo guia, debatia-se sobre não somente os anúncios serem direcionados de acordo com prioridades específicas, mas os conteúdos serem exibidos de forma personalizada e microssegmentada. Investigava-se o efeito de uma bolha informacional, na qual as mesmas convicções e ideologias transitam e se reafirmam, limitando significativamente a diversidade de opiniões e ideias. Assim, longe de serem neutros, tais mecanismos carregariam uma série de valores, conceitos e intencionalidades.

O segundo ponto de inflexão global que provocou uma reorientação do ecossistema de desinformação ocorreu em 2020, durante a pandemia de covid-19¹⁴. Naquele contexto, a Organização Mundial da Saúde

(OMS) afirmou¹⁵ que a resposta ao surto estava acompanhada por uma **infodemia**, isto é, uma superabundância de informações, algumas corretas, outras não, que dificultariam o acesso a informações e orientações confiáveis sobre o tema; a OMS também afirmava que, além da batalha contra o vírus, enfrentava-se uma batalha contra teóricos da conspiração que disseminavam desinformação, minando as respostas ao problema¹⁶. Naquele contexto, a desinformação deixava de ser tratada como fenômeno predominantemente eleitoral para tornar-se também problema de saúde pública.

Ainda em 2020, identificou-se que a manipulação da opinião pública por atores políticos através das redes sociais, longe de ser um problema produzido por atores isolados, teria ganhado escala em face da crescente organização dos atores e processos que se consolidou em torno da produção e distribuição de notícias falsas e enganosas. No *Relatório Internet, Desinformação e Democracia* do CGI.br, publicado em 2020, o termo indústria da desinformação foi empregado em referência ao “aumento contínuo da complexidade e tamanho das cadeias produtivas e redes de atores que surgiram estimuladas por altos investimentos financeiros destinados a essas atividades”¹⁷. Em mais de 80 países, ferramentas e técnicas organizadas de manipulação se

institucionalizaram como parte das campanhas políticas, constituindo-se como ameaça para a democracia em todo o mundo¹⁸.

Nos últimos quatro ciclos eleitorais brasileiros (2018, 2020, 2022 e 2024), os meios, formatos e conteúdos desinformativos não somente mudaram de padrão como se sofisticaram. A desinformação na Internet permanece como problema central para a qualidade dos processos democráticos.

Ao longo da última década, a desinformação predominante deixou de ser ancorada na **falsidade absoluta** (as chamadas *fake news*) para aproximar-se da noção de “má informação” (*malinformation*, em tradução livre) – baseada em distorções de fatos reais, omissões intencionais, exageros, recortes seletivos, comparações inadequadas e descontextualizações – compondo formas mais complexas de manipulação e ganhando efetividade. Em termos de enfoque temático, a ênfase que antes se detinha sobre adversários políticos, seus históricos e suas promessas de campanha passou a incluir com mais força o próprio **processo eleitoral**¹⁹.

Nesse curso, também mudaram os meios prioritários de circulação, de redes abertas – Facebook, em 2018 – para ambientes mais fechados – o WhatsApp, que segue sendo a principal via de difusão. A disseminação de

desinformação tornou-se mais distribuída, com circulação simultânea em múltiplas plataformas. Quanto ao formato, o vídeo passou a ser o principal vetor, quase sempre acompanhado de um texto curto que apoia e legitima a narrativa falsa²⁰.

O ano de 2025 tem sido considerado um ponto de inflexão para os conteúdos produzidos por inteligência artificial no Brasil. Até então, estes ainda não eram identificados como padrão relevante por parte das agências de checagens de informações. No ano passado, o Fórum Econômico Mundial publicou o *Relatório de Riscos Globais 2025*²¹, com o *ranking* dos principais desafios a serem enfrentados pelo mundo nos planos econômico, ambiental, geopolítico, social e tecnológico. O documento situa a desinformação como o maior perigo a curto prazo para a humanidade.

Em 2026, a popularização da **inteligência artificial (IA) generativa** tem se consolidado como um dos desafios centrais, com grande potencial disruptivo para o cenário informacional. A expansão da circulação das *deepfakes* ao longo dos últimos anos

tornou mais acessível a produção de conteúdos desinformativos com alto grau de realismo. Por esse motivo, a campanha eleitoral de 2026 tem sido apontada como uma nova etapa da desinformação eleitoral, marcada pela produção em larga escala de imagens, áudios e vídeos sintéticos.

Este guia está dividido em cinco partes. A primeira traz uma breve explicação sobre o funcionamento das plataformas digitais, em especial os sistemas de recomendação que ordenam seus conteúdos, assim como o modelo de negócios que as orienta. A segunda parte analisa questões sobre o impacto que a inteligência artificial generativa tem assumido no contexto eleitoral atual, sobretudo as *deepfakes* e os modelos de linguagem conversacionais. A terceira parte é focada em recomendações para o combate à desinformação em plataformas de redes sociais, enquanto a quarta parte traz dicas para não compartilhar ou tornar-se vítima de tais conteúdos. Por fim, a quinta parte indica fontes de informações adicionais.

Boa leitura ➔



INTERNET E PLATAFORMAS DIGITAIS



01

NESTA SEÇÃO, VOCÊ VAI ENCONTRAR:

- * Qual é a diferença entre plataformas digitais e redes sociais
- * O que é integridade da informação e desinformação
- * Uma breve explicação sobre como os conteúdos circulam em plataformas digitais
- * O que são sistemas de recomendação e quais seus impactos sobre o acesso à informação

Há vários anos, já não é possível pensar em uma cisão entre estar *online* e estar *offline* para a maior parte das pessoas. Não se faz mais necessário aguardar até o dia seguinte para receber as notícias em jornais impressos ou até aos horários delimitados pelos jornais televisivos. Ao contrário, a perda do direito à desconexão já é amplamente reconhecida, uma vez que *smartphones* parecem ter se tornado extensões de nossas mãos.

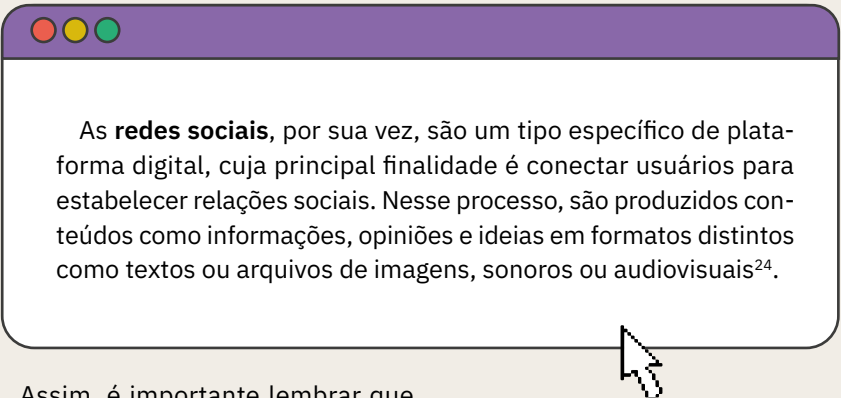
Hoje, é por meio de plataformas digitais que os usuários de Internet brasileiros acessam informações sobre o que está acontecendo no mundo, no país ou na cidade. Para 60% dos usuários de Internet com 16 anos ou mais, o principal meio utilizado são aplicativos de mensagens, seguidos por *feeds* de vídeos curtos (53%), *sites* ou aplicativos de vídeos (50%) e *feeds* de notícias em redes sociais (46%)²².

PLATAFORMAS DIGITAIS OU REDES SOCIAIS? ENTENDA A DIFERENÇA



As **plataformas digitais** integram um escopo mais amplo do que o das redes sociais. Incluem também, por exemplo, aplicativos de mensageria privada, mecanismos de buscas, plataformas de conteúdos gerados pelos usuários, como vídeos, e de conteúdos sob demanda, como *streamings*.

O que são plataformas digitais? São sistemas que operam sobre a infraestrutura digital e têm como função intermediar relações entre diferentes atores²³. Podem conectar, por exemplo, fornecedores de serviços e produtos a consumidores e usuários. Algumas das características marcantes das plataformas são o uso intensivo de dados, os efeitos de rede e, com frequência, o emprego de tecnologias de inteligência artificial.



As **redes sociais**, por sua vez, são um tipo específico de plataforma digital, cuja principal finalidade é conectar usuários para estabelecer relações sociais. Nesse processo, são produzidos conteúdos como informações, opiniões e ideias em formatos distintos como textos ou arquivos de imagens, sonoros ou audiovisuais²⁴.

Assim, é importante lembrar que, na Internet, o ecossistema informacional é mais amplo que o das redes sociais e inclui várias outras categorias de plataformas, além da *Web* — onde estão os *sites* — e de outros serviços e aplicações que compõem a camada de aplicações.

No primeiro guia²⁵, vimos que o termo “notícia falsa” vinha caindo em desuso, uma vez que se identificava a existência de um fenômeno mais amplo em curso, denominado de **desinformação**. Esta inclui não somente notícias falsas, mas, por exemplo, a publicação proposital de uma notícia antiga ou fora de contexto e outros tipos de conteúdos falsos ou enganosos que não necessariamente assumem o formato de notícia.

Em 2026, os estudos realizados por agências de checagem de fatos têm confirmado essa tendência crescente nos conteúdos²⁶, com a prevalência de informações manipuladas de diversas formas, fugindo do padrão restrito à falsidade absoluta e adquirindo mais nuances.

Mais recentemente, no debate sobre o enfrentamento à desinformação, tem se destacado o conceito de **integridade da informação** — que se refere à precisão, consistência e confiabilidade da informação²⁷. O Brasil, em 2024, apresentou manifestação na Cúpula do G20 propondo que a integridade da informação fosse um princípio e um dever de todos os Estados, sendo, portanto, necessário discutir caminhos multilaterais para o aprimoramento do ambiente digital²⁸.

Adotar a abordagem da integridade da informação traz algumas vantagens, como ir além da ótica reativa da remoção de conteúdos. Passa-se a considerar não somente o resultado final, mas as dinâmicas algorítmicas e estruturais associadas à circulação de informações. O foco passa a ser proativo: direcionado para a implementação de medidas que promovam um ecossistema informacional sustentável e plural²⁹.

Como vimos no primeiro guia, as plataformas digitais estão longe de ser consideradas apenas um **meio neutro** por onde circulam as informações, e há um conjunto de motivos para isso. Ainda que muitas delas sejam gratuitas e pareçam espaços públicos neutros, são oferecidas por empresas privadas que possuem seus próprios interesses econômicos e políticos, que integram o *design* dos serviços que oferecem. O modelo de negócios dessas empresas é fundamentado na venda de publicidade direcionada, e isso impacta diretamente os padrões de circulação de seus conteúdos.

O que isso significa?
Que o problema da desinformação vai muito além do uso impróprio por parte de pessoas mal-intencionadas que estariam nessas plataformas.

As próprias plataformas moldam de forma intencional as experiências dos usuários a partir da forma como são desenhadas. Assim, elas não se resumem a um reflexo do mundo social que está em seu entorno, mas contribuem para moldar esse mundo, e,

além disso, ampliam a escala e a velocidade dos processos que ali ocorrem.

Antes de falarmos sobre a criação de conteúdos desinformativos na Internet, cabe explorarmos um pouco as condições de produção desse fenômeno.

Quais estímulos e fatores técnicos podem ter contribuído para mudanças no comportamento das pessoas? Para começar essa conversa, vamos tratar de uma das principais mudanças que afetaram o fluxo de informações na Internet nos últimos anos: o uso de algoritmos para a distribuição de conteúdos nas plataformas.

De acordo com a *Tipologia de Provedores de Aplicação* elaborada pelo CGI.br, as plataformas de redes sociais devem ser classificadas como **aplicações que exercem alta interferência sobre os conteúdos** gerados pelos seus usuários, o que se deve a uma série de funcionalidades que as integram. Uma das mais relevantes são os **sistemas de recomendação** de conteúdos.

Ao longo dos anos, as principais redes sociais passaram por mudanças infraestruturais relevantes, aumentando a própria capacidade de intervenção no que ali circula. As principais redes sociais utilizadas no início do século XXI ofereciam funcionalidades básicas, como a criação de perfis pessoais que podiam se interconec-

tar formando redes de amizades. A partir de 2006, foram gradualmente introduzidos os *feeds* de notícias, que eram ordenados cronologicamente. Os conteúdos que circulavam ali eram determinados a partir da escolha ativa de cada usuário sobre quais contas iriam seguir. Esse modelo foi gradualmente substituído pela curadoria algorítmica, ordenada com base em previsões personalizadas, com base em técnicas de perfilamento e microdirecionamento³⁰.

Essa mudança aconteceu junto com o advento do que se convencionou chamar de *Big Data*. Trata-se de um processo de datificação da vida (transformação de todos os aspectos da nossa vida em dados) e da coleta e tratamento desses dados que passaram a formar bases de dados gigantescas e utilizadas para a criação de perfis individualizados³¹.

Em termos práticos, esses sistemas funcionam da seguinte forma: ao **coletar** o máximo de informações dos usuários, como idade, localização, contas seguidas, históricos de navegação, bem como métricas de engajamento, como curtidas, conteúdos visualizados e tempo de permanência na aplicação, muitas dessas plataformas ganharam capacidade de **inferir** características e interesses, bem como tentar prever comportamentos dos usuários. Com base nos perfis que são identificados, pode-se definir quais conteúdos e

anúncios serão mostrados, para quem e com que prioridade, com efeitos concretos e cada vez mais precisos na modulação do comportamento de usuários, principalmente no aumento do tempo de engajamento nessas aplicações.

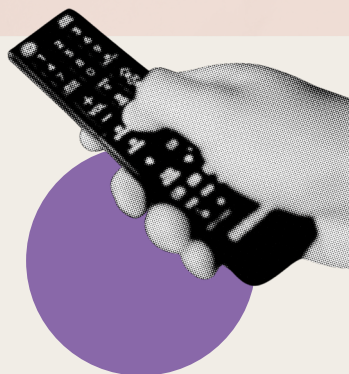
Durante o processo de **tratamento** de dados, mesmo informações que não foram explicitamente fornecidas podem ser inferidas, como interesses prováveis, hábitos de consumo ou afinidades com determinados temas. Você já teve a sensação de que, às vezes, parece que o algoritmo leu seus pensamentos? Isso se deve ao grau de precisão e sofisticação que esses sistemas podem atingir, o que é possível graças ao volume massivo de informações coletadas. É por isso que eles são tão valiosos sob o ponto de vista do mercado.

Ao mesmo tempo, na medida em que são priorizadas métricas de **engajamento**, são criados incentivos para a disseminação de informações que possam reter mais atenção dos usuários e amplificar a viralização dos conteúdos — o que faz com que se tornem economicamente mais rentáveis. Dessa forma, conteúdos mais sensacionalistas, ou que mobilizam emocionalmente os usuários, se tornam mais estratégicos do que a qualidade da informação, tornando-se um terreno fértil para a disseminação de conteúdos desinformativos³².

Uma consequência dessa mudança na dinâmica informacional para as eleições foi a adoção de estratégias de comunicação baseadas na segmentação para diferentes perfis de potenciais eleitores, principalmente a partir de 2018 no Brasil. **Essas estratégias passaram a substituir o padrão comunicacional único voltado ao público amplo, como aquele tradicionalmente veiculado pela propaganda eleitoral televisiva.**

Ao adotar essa estratégia, um mesmo candidato poderia assumir diferentes formas, a partir das aspirações de seus apoiadores, criando uma espécie de caleidoscópio ou mosaico. Diferentes perfis de eleitores enxergariam nele diferentes projetos³³, que se conectariam parcialmente a demandas particulares e afinidades latentes, como interesses, medos e outros afetos³⁴.

O problema do ponto de vista informacional é que, conforme tais conteúdos são direcionados para públicos restritos, afastados da ampla visibilidade pública e com pouca transparência sobre o conteúdo e os critérios adotados, se criam dificuldades relevantes para a supervisão e fiscalização, além de dificultar o controle social sobre a atuação dos candidatos em períodos eleitorais.



Os sistemas de recomendação, de forma ampla, têm assumido um papel central no fluxo de informações contemporâneo. São operacionalizados por algoritmos que fazem uma curadoria dos conteúdos postados por usuários: ordenam, filtram e priorizam conteúdos de terceiros sob critérios norteados pelo aumento do engajamento e baseados na coleta e no tratamento massivo de dados³⁵. Isso faz com que o problema seja não somente a produção de conteúdos danosos, mas a sua amplificação, produzindo efeitos profundos na esfera pública.

Em **mecanismos de busca**, também houve mudanças estruturais significativas, intermediadas por algoritmos, que impactaram no ranqueamento dos resultados de cada pesquisa realizada. Os usuários passaram a visualizar anúncios com base nos interesses expostos nas pesquisas que realizavam nos serviços, em um modelo baseado em estratégias sofisticadas de perfilamento e microdirecionamento, que se tornou a principal fonte de receita. Atualmente, os resultados que aparecem no topo dos mecanismos de buscas não são orientados somente por critérios associados à qualidade da informação, relevância ou credibilidade da fonte, mas a incentivos financeiros, o que trouxe fortes impactos sobre o acesso à informação³⁶.

Se até 2022 a desinformação na Internet foi potencializada sobretudo por automação, disparos coordenados e arquiteturas algorítmicas, nas eleições seguintes a IA generativa foi gradualmente passando a integrar o rol de preocupações³⁷. O conjunto de técnicas que compõe o campo da IA, portanto, é significativo para o ecossistema da desinformação na Internet ao menos desde 2018, ainda que as técnicas predominantes e os padrões mudem a cada ciclo eleitoral. Em 2026, a IA generativa tem sido considerada o tema do ano. É este o tema que será explorado no próximo capítulo.

ELEIÇÕES, DEMOCRACIA E INTERNET: O DESAFIO DA IA GENERATIVA



Compartilhar



02

NESTA SEÇÃO, VOCÊ VAI ENCONTRAR:

- * O que é IA generativa, conteúdo sintético e *deepfake*
- * Quais os impactos das *deepfakes* nas decisões eleitorais
- * O uso de *deepfakes* em casos de violência política de gênero
- * Os impactos do uso de *chatbots* como fonte de informações eleitorais



As disputas eleitorais deixaram de se restringir a projetos políticos: há uma questão técnica que tem se consolidado como um dos vetores centrais para as campanhas. O controle das infraestruturas digitais tem atravessado as estratégias de cada candidato, por sua capacidade de trazer visibilidade, reorganizar as narrativas, moldar a opinião pública e influenciar as adesões. Se essa tendência já vinha se consolidando, a disponibilidade de *deepfakes* mais sofisticadas acrescentou novos elementos à disputa.

Observando o contexto mais amplo, a desinformação e as consequências adversas das tecnologias de IA foram apontadas como um dos **principais riscos globais** de 2026³⁸. Cerca de 81,2% dos casos de desinformação com IA identificados por veículos de checagens surgiram apenas nos últimos dois anos³⁹. Um dos principais motivos para isso é o aprimoramento e a ampla disponibilidade da IA generativa.

O QUE É IA GENERATIVA?

A **IA generativa** é um tipo de inteligência artificial capaz de criar novos conteúdos, como textos, imagens, vídeos, áudios e até códigos de *software*. Vem daí o nome “generativa”: dessa capacidade de gerar. Para que isso seja possível, esses sistemas dependem de grandes volumes de informação, a partir dos quais identificam padrões, produzindo com a maior precisão possível um conteúdo novo baseado em métodos probabilísticos⁴⁰.

Na prática, talvez o tipo de IA generativa que vem sendo utilizado de forma mais rotineira são os chamados *chatbots* ou sistemas conversacionais (como o ChatGPT, Gemini e Claude). Eles funcionam assim: através de uma estrutura de probabilidades, produzem a sequência de texto que estatisticamente seria mais parecida com a de um ser humano, replicando a nossa linguagem.



Isso é tão bem feito que pode dar a impressão de que estamos de fato conversando com uma pessoa. No entanto, é fundamental entender que esses sistemas não compreendem de fato contextos, significados e experiências tal como um humano é capaz de fazer. Aliás, há uma farta quantidade de pesquisas que identificam erros e vieses⁴¹ nos resultados produzidos, inclusive sobre informações relacionadas a candidatos e partidos políticos.

Há também outros usos de IA generativa além de textos. Alguns sistemas são capazes de produzir imagens e vídeos (por exemplo, editando e manipulando imagens, criando avatares digitais e *deepfakes*), voz (para geração de música, efeitos sonoros e clonagem de voz), códigos e interfaces, sendo bastante úteis para vários setores da sociedade.



O QUE É **CONTEÚDO SINTÉTICO?**

Trata-se de um termo técnico amplo, que se refere a qualquer conteúdo produzido artificialmente ou manipulado, ou seja, que não provém diretamente de um dado real. Podem ser imagens, vídeos, áudios e outros materiais. Esses conteúdos podem ser criados através de diversas ferramentas e técnicas; no caso específico de *deepfakes*, as técnicas utilizadas são de IA generativa⁴². Assim, as *deepfakes* são um subgrupo dentro dos conteúdos sintéticos.

Nos últimos anos, as *deepfakes* se tornaram mais acessíveis, baratas e convincentes, tornando a distinção entre conteúdos autênticos e sintéticos progressivamente mais difícil. Sob o ponto de vista técnico, isso se deve a alguns fatores principais, como a ampla disponibilidade de dados na Internet, que também contribuiu para o aprimoramento de algoritmos capazes de mapear automaticamente características biométricas⁴³.

Adicionalmente, com a maior necessidade de detectar falsificações, as técnicas desenvolvidas para detecções forenses passaram a contribuir para o ciclo de aprendizado contínuo e para a correção de falhas. Assim, se antes se demandava um alto volume de dados e capacidade de processamento para criar conteúdos realistas, os avanços nos modelos têm ampliado bastante a capacidade de geração de imagens e vídeos⁴⁴.

Desde as eleições de 2024, os riscos da IA generativa foram se destacando como ameaça à integridade do processo democrático⁴⁵. Em aproximadamente 80% dos países com eleições competitivas em 2024, a IA generativa foi utilizada para a produção de conteúdos sintéticos em campanhas de desinformação⁴⁶, tendo sido apontada como o terceiro maior risco global. No ano anterior, a campanha presidencial na Argentina foi a primeira na região que fez uso de IA em

ampla escala, sobretudo com a criação de vídeos *deepfakes* que viralizaram em diversas plataformas⁴⁷. Casos semelhantes foram identificados em diversos países, destacando-se o caso da Eslováquia⁴⁸.

I. O USO DE DEEPPAKES EM CONTEXTO ELEITORAL

O QUE SÃO DEEPPAKES?

Deepfakes são conteúdos — como áudios, fotos e vídeos — modificados ou artificialmente criados por meio de inteligência artificial, para simular a voz ou a aparência de uma pessoa real, sendo um tipo de mídia sintética.

Ainda há, na literatura científica, um debate sobre o limite do que é considerado ou não, uma vez que há diferentes graus de manipulação que podem ser realizados em um conteúdo^{49 50}.

As eleições de 2022 foram as primeiras na história brasileira em que o acesso a tecnologias para a produção de *deepfakes* esteve amplamente disponível, ainda que o resultado final, muitas vezes, fosse de baixa qualidade⁵¹. Desde então, o uso de *deepfakes* tem se alastrado, passando de

tecnologia emergente para se instalar de forma perene no ambiente da desinformação digital⁵², não somente em grupos fechados à margem das campanhas oficiais, mas sendo incorporado como ferramenta por várias delas⁵³.

Foi nesse contexto que, em 2024, o Tribunal Superior Eleitoral (TSE) adotou uma série de normas para o uso de IA na propaganda eleitoral, situando o Brasil como um dos primeiros a adotar uma regulamentação eleitoral com este foco⁵⁴. Com a **Resolução n. 23.732/2024**⁵⁵, permite-se o uso de IA na propaganda eleitoral, desde que com transparência, exigindo-se que tais conteúdos sejam identificados de forma visível, mediante recursos como marcas d'água.



Já em 2026, o uso de inteligência artificial mais uma vez esteve no cerne das novas regras aprovadas pelo TSE para propaganda eleitoral, com a publicação da **Resolução n. 23.755/2026**⁵⁶. Nesse novo regramento, a medida central foi a **proibição** de publicar, republicar e impulsionar novos conteúdos produzidos ou alterados por IA dentro de uma **janela temporal** específica – no período compreendido entre as 72 horas que antecedem e as 24 horas que sucedem cada turno da votação. A medida, cabe destacar, inclui mesmo aqueles conteúdos que estejam rotulados, mas vale somente para conteúdos novos, e não para aqueles que já estavam em circulação.

A resolução também prevê três proibições específicas para o uso de IA:

- Para fabricação ou manipulação conteúdos que difundam fatos notoriamente inverídicos ou descontextualizados;
- Para a criação de *deepfakes* para alterar ou substituir a imagem ou voz de uma pessoa viva, falecida ou fictícia, com fins eleitorais; e
- Para o uso de *chatbots* ou avatares para simular a interlocução com avatares ou pessoas reais.

O objetivo dessa medida é evitar que, durante o período mais crítico do processo eleitoral, tais conteúdos circulem em alta velocidade e gerem danos sem tempo hábil para a medida de mitigação adequada. Também parte de um diagnóstico: há momentos, no processo eleitoral, de maior vulnerabilidade, em que o dano informacional pode ser irreversível⁵⁷. A eficácia da medida será testada pela primeira vez nas eleições de 2026, considerando que há desafios técnicos relevantes para a sua implementação.

AS DEEPFAKES IMPACTAM OU NÃO IMPACTAM AS DECISÕES ELEITORAIS?

A preocupação que tem sido mais apontada em relação às *deepfakes* diz respeito ao **realismo ou à fidedignidade**. Com o aprimoramento constante, mesmo eleitores experientes em avaliar conteúdos produzidos por IA podem ter dificuldades de identificar se um conteúdo é verdadeiro ou não.

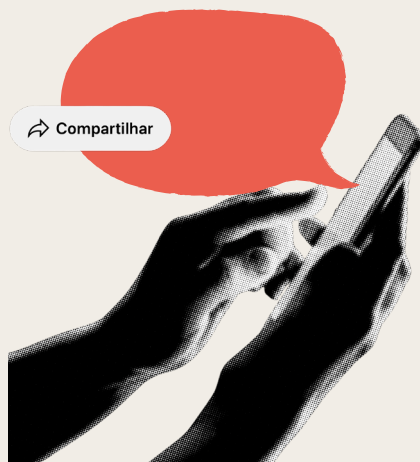
Isso coloca dois desafios centrais: (1) o risco de não saber que determinado conteúdo é enganoso, o que produz efeitos danosos; e (2) a desconfiança generalizada sobre qualquer tipo de informação, mesmo as verdadeiras. Ambos afetam de forma relevante o ecossistema informacional. A perda de confiança em instituições como a imprensa e o Judiciário, somada à polarização política, também contribuem para esse cenário, fazendo com que convicções pessoais se sobreponham à verificação dos fatos⁵⁸.

Há ainda outras dimensões relevantes ao considerar o impacto de *deepfakes* em cenários eleitorais. Em um contexto em que a exposição a notícias nas plataformas digitais é seletiva, afetada pelos mecanismos de recomendação de conteúdo, o padrão de consumo informacional mais comum é aquele no qual os eleitores consomem apenas informações que confirmam o que já pensam. Quando se deparam com informações que contrariam essas crenças, tendem a descartá-las — a chamada racionalidade motivada. Nesse sentido, podem produzir o efeito de **reforço ideológico**⁵⁹.

É importante considerar que a adesão do eleitor é determinada por um conjunto de fatores, como afetos, identidades e convicções ideológicas, o que faz com que dificilmente determinadas notícias tenham a capacidade de **converter drasticamente** a vontade de um eleitor — sejam elas falsas, verdadeiras ou *deepfakes*⁶⁰. Isso não significa, no entanto, que a exposição contínua à desinformação não produza efeitos relevantes. Afinal, ela contribui para sedimentar dúvidas a respeito de determinados consensos e a reenquadrar problemas sociais, redefinindo o senso comum⁶¹. Isso pode ser especialmente relevante em contextos de eleições acirradas, com amplo número de indecisos.

A exposição a conteúdos desinformativos, como as *deepfakes*, pode contribuir, por um lado, para a percepção de conhecimento político e para agregar as pessoas em torno da campanha, **impulsionando a mobilização e o engajamento**. Por outro, quanto ao público mais amplo e especificamente ao grupo visado pelas publicações, a desinformação pode contribuir para o **silenciamento**, diminuindo a disposição de agir⁶². Em qualquer uma das situações, esses conteúdos contaminam o espaço público de debates e o acesso à informação, elementos que são vitais para processos democráticos.

Com cada vez mais frequência, **influenciadores digitais**⁶³ têm assumido papel estratégico no debate político⁶⁴, passando a mobilizar uma audiência que os canais jornalísticos tradicionais de comunicação não têm capacidade de mobilizar, o que gera consequências relevantes para a polarização e para a circulação de conteúdo desinformativo⁶⁵. Pela lei eleitoral⁶⁶, candidaturas estão impedidas de contratar ou oferecer qualquer tipo de benefício a influenciadores em troca da realização de *marketing* de influência político/eleitoral. No entanto, ainda há um conjunto de condutas que, embora não sejam ilegais, podem ser prejudiciais ao debate democrático. Ainda que sejam capazes de produzir amplos impactos, não há qualquer tipo de regulamentação



sobre as atividades dos influenciadores, enquanto, por exemplo, os canais jornalísticos são regidos pelos princípios éticos da atividade jornalística e por regulação específica⁶⁷.

Um fenômeno que tem se destacado em 2026 é o dos **influenciadores digitais sintéticos**, que não se baseiam em pessoas reais, mas emulam supostos eleitores, influenciadores, apresentadores, comentaristas e lideranças populares, e nem sempre há informação explícita de que se trata de IA⁶⁸. A maior parte dos casos mapeados funcionam como vetores de desinformação política, apresentando conteúdos com alegações enganosas. Em termos de alcance, interação e nível de engajamento, alguns desses perfis possuem números semelhantes aos de políticos influentes de diferentes espectros⁶⁹.

Há um risco já mapeado desses avatares que está em outra camada. Ainda que se saiba tratar-se de conteúdo sintético, a exposição a conteúdos com fortes componentes emocionais, em especial a raiva e indignação, pode produzir efeitos relevantes em termos de mobilização. A exposição reiterada também contribui para a naturalização dos discursos desses perfis, que passam a ser tratados como eleitores comuns indignados com a situação do país, o que produz impactos discursivos semelhantes ao de pessoas reais⁷⁰.

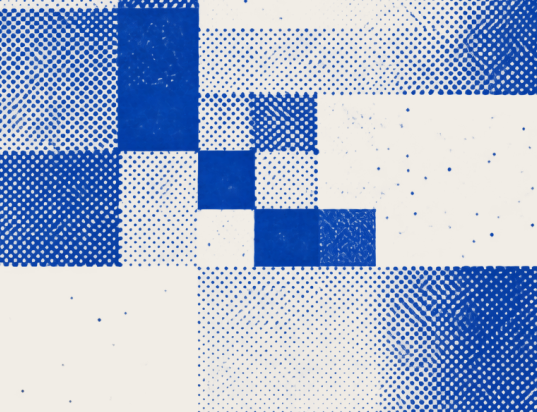
Com frequência, a produção de conteúdos sintéticos se baseia na apropriação da imagem de jornalistas e de veículos de comunicação tradicionais, como forma de emular a credibilidade jornalística para disseminar desinformação, aprofundando a sua capacidade de impacto⁷¹. Na condição de figuras públicas, jornalistas se encontram entre os alvos preferenciais de *deepfakes* — dos quais 74% são mulheres⁷².

Em 2026, alguns perfis e até campanhas oficiais têm adotado o uso de *deepfakes* não em contexto de falsabilidade, mas como recurso representacional, sinalizando explicitamente tratar-se de uma simulação. Dessa forma, pode-se trazer à presença figuras políticas ausentes⁷³ ou que sequer

existem⁷⁴. Isso levanta outra questão: saber que os conteúdos não são reais ameniza os seus efeitos?

Como vimos, a inteligência artificial facilitou a capacidade de reconstruir de forma fidedigna a imagem, a fala e os gestos de uma pessoa, produzindo momentos que nunca aconteceram. No caso de uma liderança, isso significa que ela pode continuar aparecendo, falando, mobilizando apoiadores e intervindo no presente ainda que seu corpo não esteja disponível para participar da disputa, transformando o sentido de representação e participação política⁷⁵.

Isso gera riscos de aprofundamento nas assimetrias na disputa, a depender da capacidade de cada grupo de mobilizar a infraestrutura técnica, os recursos organizacionais e a contratação de pessoal especializado, o que afeta o investimento financeiro necessários para a produção, disseminação e impulsionamento desses conteúdos. Assim, o uso de *deepfakes* nas eleições, mais do que uma questão de transparência sobre a distinção entre verdadeiro e falso, oferece o risco de aprofundar a desigualdade nas capacidades de produzir presença, visibilidade e influência política, prejudicando o equilíbrio da disputa democrática⁷⁶.



VIOLÊNCIA POLÍTICA DE GÊNERO E DEEPFAKES

Ainda que a preocupação com os impactos políticos e desinformativos do uso de *deepfakes* tenha se destacado no debate público nos últimos anos, há estudos que apontam que o tipo mais prevalente de *deepfakes* em circulação na Internet é de natureza sexual⁷⁷.

Dentre os vídeos com *deepfakes* em circulação entre 2019 e 2023, 98% são de conteúdos pornográficos, dos quais 99% retratam mulheres⁷⁸ dentre os modelos disponíveis para *download* público, 96% têm como alvo mulheres⁷⁹, demarcando um forte componente de gênero. Quanto aos alvos, a maior parte pertence à esfera pública, como celebridades, políticas e jornalistas⁸⁰.

O ecossistema de criação e disseminação de *deepfakes* de conteúdo íntimo vem se modificando rapidamente nos últimos anos, compondo uma cadeia ampla e interconectada que não se restringe a um só modelo, aplicativo ou *website* e agrega diversos tipos de tecnologias⁸¹.

Na prática, a produção de *deepfakes* íntimas não consensuais, hoje, é acessível a qualquer usuário que não possua conhecimento técnico especializado, bastando uma imagem facial nítida; elas podem ser produzidas em poucos minutos, com qualidade e de forma gratuita.



A facilidade de acesso e a ampla disseminação desses recursos contribuem para naturalizar uma prática que se constitui como violência sexual contra mulheres, o que já é reconhecido pela legislação brasileira. Em períodos eleitorais, essas práticas passaram a integrar os casos de violência política de gênero contra candidatas, com vários episódios documentados nas eleições municipais de 2024⁸².



O QUE É **VIOLÊNCIA POLÍTICA DE GÊNERO?**

Trata-se de toda ação, conduta ou omissão que tenha como objetivo impedir, atrapalhar ou restringir o pleno exercício dos direitos políticos das mulheres. Pode atingir candidatas, pré-candidatas, eleitas e mulheres que exercem representação pública ou política, e ocorrer tanto no ambiente físico como no digital⁸³.

O recurso de *deepfakes* e montagens tem sido utilizado recorrentemente como estratégia para constranger, humilhar e desqualificar candidaturas femininas⁸⁴. Junto a outras práticas que ocorrem em ambiente digital, como assédio, ameaça, vazamento de dados sensíveis, perseguição e chantagem, esse recurso contribui para desencorajar a atuação política de seus alvos⁸⁵.

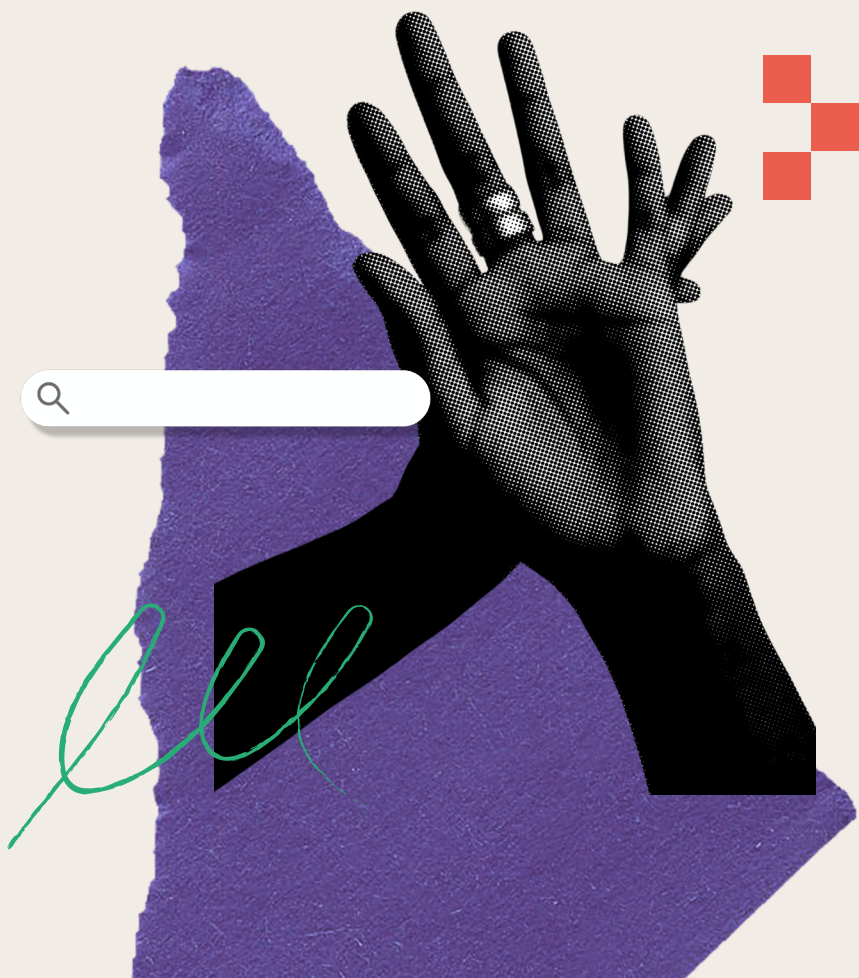
Nos últimos anos, tem-se observado um padrão, no qual mulheres candidatas recebem mais do que o dobro de ofensas em relação aos homens na Internet; ainda, **mulheres negras** são as maiores vítimas de violência política de gênero e raça, representando 87% dos casos ocorridos em ambiente digital – sendo 71% delas parlamentares em exer-

cício. Além disso, outros marcadores também contribuem para o agravamento de tais violências e fazem com que o ambiente político se torne especialmente inóspito para mulheres negras, LGBTQIAPN+, periféricas e com deficiências.

É com base em tais preocupações que o CGI.br publicou uma *Nota pública sobre exploração sexual por uso indevido de inteligência artificial generativa*⁸⁶, recomendando que empresas que oferecem serviços de geração de imagens por IA, bem como as lojas de aplicativos e as plataformas que difundem e dão acesso a esse tipo de ferramenta ou conteúdo, atuem de modo proativo para estabelecer mecanismos de proteção adequados. Também produziu uma nota técnica com recomendações regula-

tórias indicando a vedação de sistemas de IA que possibilitem a produção ou disseminação ou facilitem a criação de materiais com cena de nudez ou conteúdo sexual sem consentimento⁸⁷. E, ampliando o escopo analítico, produziu uma *Nota técnica sobre Violência de Gênero em Ambientes Digitais*⁸⁸.

Em 2026, como resposta às preocupações sobre o avanço de *deepfakes* de conteúdo sexual, a resolução do TSE para propaganda eleitoral passou a **proibir**, aos provedores de aplicação, a oferta de sistemas de inteligência artificial (ou tecnologia equivalente) que criem ou alterem fotografias, vídeos ou outros registros audiovisuais que contenham cena de sexo, nudez ou pornografia envolvendo candidata ou candidato. Também se passou a proibir publicidade eleitoral que represente ato de violência política contra a mulher.



II. O USO DE CHATBOTS COMO FONTE DE INFORMAÇÕES ELEITORAIS

As ferramentas de IA generativa, em especial os *chatbots*, têm se expandido rapidamente como intermediárias da informação⁸⁹. Diferentemente dos mecanismos tradicionais de buscas, que localizam e direcionam os conteúdos para fontes específicas, há um processo de sintetização, reorganização e apresentação das informações em forma de linguagem conversacional ajustada ao usuário⁹⁰, produzindo um grau de intermediação mais profundo. Sob o ponto de vista do usuário, trata-se de um mecanismo prático e personalizado; no entanto, ao emular com precisão conteúdo interativo, informativo e influente, esses sistemas possuem maior capacidade persuasiva e pouca transparência.

Ainda que o tema das *deepfakes* venha dominando o debate público sobre os riscos da IA, um estudo recente apontou que textos gerados por inteligência artificial convencem mais do que *deepfakes*, podendo ser considerados mais confiáveis pelo público do que informações verificadas⁹¹. O risco também aumenta para o caso dos sistemas conversacionais,

que mantêm conversas personalizadas com cada usuário. Em contraste, alguns experimentos sobre desinformação visual apontam para um aumento da desconfiança em relação a imagens e vídeos gerados por IA, ainda que a capacidade de identificar se o conteúdo é sintético ou não permaneça como desafio.

Já há pesquisas consistentes que identificam, na interação com *chatbots* de forma ampla, a presença de conteúdos desinformativos e vieses discriminatórios de diferentes naturezas^{92 93 94}, inclusive políticos⁹⁵. Além disso, são capazes de influenciar a opinião de eleitores, produzindo efeitos mais profundos do que campanhas e propagandas convencionais⁹⁶ e maior grau de persuasão do que pessoas em debates *online*⁹⁷. Também foram identificados riscos significativos de radicalização política e recrutamento *online* de larga escala associados a modelos de linguagem⁹⁸.

Como forma de responder a esses riscos, a Resolução n. 23.755/2026⁹⁹ sobre propaganda eleitoral também trouxe a vedação de que provedores

de IA recomendem, ranqueiem, sugiram ou priorizem candidatos, campanhas, partidos, federações ou coligações, bem como veda a emissão de opiniões ou qualquer forma de favorecimento ou desfavorecimento político-eleitoral. Essa medida parte da preocupação com que a interação com esses sistemas interfira, direta ou indiretamente, no processo decisório sobre o voto.

No entanto, mesmo com a proibição, identificou-se que as IAs seguiram apresentando algum grau de ranqueamento ou priorização de candidatos em 90% das respostas sobre temas eleitorais. Também foram identificados casos de imprecisão factual em diferentes ferramentas, as chamadas “alucinações”, mesmo em respostas aparentemente bem fundamentadas¹⁰⁰.



COMO COMBATER DESINFORMAÇÃO NAS ELEIÇÕES



03

NESTA SEÇÃO, VOCÊ VAI ENCONTRAR:



Diretrizes a serem observadas no combate à desinformação durante as eleições

Este capítulo trata das *Diretrizes para Regulação de Plataformas de Redes Sociais*, publicadas pelo *CGI.br*¹⁰¹. Para este guia, foram selecionadas nove entre as que mais se relacionam ao tema do combate à desinformação em períodos eleitorais. Para maior aprofundamento, indicamos a leitura das 46 diretrizes na publicação completa.



Diretriz 4

Promover medidas contra interferência indevida em processos eleitorais-democráticos

As plataformas de redes sociais devem estabelecer mecanismos para detectar e mitigar riscos de interferência indevida na integridade de processos democráticos, inclusive em eleições. Incluem-se:

- Vedar e monitorar práticas como monetização, recomendação e impulsionamento e anúncios de conteúdo antidemocrático e de canais contumazes ou recorrentes nesse tipo de conteúdo e a contratação de disparos em massa em rede social de mensagens;
- Vedar, em contexto eleitoral, estratégias de uso enganoso de mecanismos de buscas; e
- Monitorar e mitigar riscos de cibersegurança, como invasão ou comprometimento de contas e perfis de participantes de processos eleitorais, democráticos ou institucionais do Estado brasileiro.

Diretriz 10

Estabelecer mecanismos e procedimentos de transparência para assegurar a integridade de campanhas e processos eleitorais que ocorram nas redes sociais

As plataformas de redes sociais devem reforçar seus mecanismos de transparência em períodos eleitorais, com atenção especial aos meios de ampliação da circulação de conteúdos, incluindo seus mecanismos de recomendação e impulsionamento de conteúdos.

Nesses períodos, as plataformas devem fornecer informações detalhadas e com granularidade em suas bibliotecas de anúncios e sobre os demais sistemas e políticas relevantes ao contexto eleitoral. As plataformas deverão manter repositório de anúncios de cunho político-eleitoral, inclusive aqueles que forem porventura não disponibilizados ao público, por período determinado, após o qual ainda caberá às plataformas preservar indicadores agregados do conjunto dos anúncios, mesmo que se descarte o conteúdo individual de cada anúncio.

Diretriz 32

Proibir perfilamento com base em dados sensíveis

As plataformas de redes sociais (assim como outros controladores de dados) não podem utilizar dados sensíveis com a finalidade de perfilamento para publicidade e impulsionamento, sem a obtenção de consentimento do titular de dados de forma específica e destacada e para finalidades específicas. Isso significa que eventual consentimento, para ser válido, além de precisar ser livre, informado e inequívoco, não pode ser fornecido de forma genérica, como em meio aos termos de uso ou política de privacidade. Ainda, em linha com o princípio 3 (“Autodeterminação informacional”) do CGI.br para regulação de redes sociais, a manifestação de consentimento deve ser exercida sem prejuízo no acesso ao serviço, especialmente considerando a dominância e essencialidade de algumas plataformas de redes sociais.

Ademais, para fins de perfilamento, a regulação deve proibir o compartilhamento de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica, conforme prerrogativa estabelecida pela LGPD à autoridade reguladora.

Para além do cumprimento estrito da LGPD, a regulação deve vedar a utilização de técnicas de perfilamento para direcionamento de publicidade comercial, bem como o emprego de análise emocional, de realidade aumentada, de realidade estendida e de realidade virtual para perfilamento e direcionamento de publicidade comercial.

Diretriz 33

Assegurar possibilidade de escolha do usuário sobre a curadoria e recomendação de conteúdo, incluindo opção de uso sem perfilamento algorítmico

As plataformas de redes sociais devem permitir que os usuários exerçam escolhas sobre as recomendações de conteúdo ou publicidade que lhes serão destinadas. Isso deve incluir a possibilidade de desativação de qualquer curadoria e recomendação de conteúdo direcionada a partir do perfilamento feito com base nos dados pessoais de usuários.

Exemplos de ferramentas relevantes para a efetividade de tais escolhas são a opção de *feeds* cronológicos ou distribuídos por critérios não comportamentais, como os assuntos de interesse definidos por cada usuário ou as pessoas seguidas por ele.

Além disso, as plataformas de redes sociais devem explicar os diferentes critérios de recomendação, a implicação de cada escolha e o funcionamento dos mecanismos de curadoria e recomendação de conteúdo.

Atentando-se ao princípio da autodeterminação informacional — que engloba a ideia de minimização da coleta de dados —, a coleta de dados pessoais de usuários que optaram pela não personalização algorítmica deve ser feita apenas quando estritamente necessário para atender finalidades legítimas, consoante o disposto na LGPD.



Diretriz 7

Estabelecer mecanismos e procedimentos de transparência na recomendação e monetização de conteúdo

As plataformas de redes sociais devem garantir publicidade acerca dos parâmetros de recomendação¹⁰² de conteúdo e esclarecer como as configurações de personalização escolhidas pelos usuários impactam a curadoria a eles exibida. Em outras palavras, os usuários têm o direito de conhecer por quê e como os conteúdos lhes são direcionados.

No mesmo sentido, as plataformas de redes sociais devem ser transparentes quanto aos critérios utilizados para que o conteúdo seja elegível para monetização e como tal monetização ocorre.

A autoridade reguladora deve definir as hipóteses em que a disponibilização de informações ao público geral é obrigatória, e aquelas em que essas informações podem ser fornecidas apenas à autoridade reguladora. Exemplos deste último caso são informações que violem segredo comercial ou industrial e proteções de propriedade intelectual, ou que prejudiquem a operação segura do serviço. Nessas

situações, a autoridade reguladora deverá buscar definições e critérios que não firam os direitos de informação dos usuários.

Diretriz 36

Interromper a monetização de conteúdos desinformativos com maior potencial de gerar danos a terceiros

A regulação deve contemplar obrigações para que as plataformas de redes sociais previnam danos gerados por conteúdo desinformativo monetizado em seus ambientes, tais como danos relacionados à desinformação climática, ao funcionamento do processo político democrático, à saúde pública etc.

Essas obrigações devem abarcar disposições que vedem a monetização de tais conteúdos enganosos nos casos em que exista um maior potencial de gerar danos a terceiros. A identificação do conteúdo desinformativo deve contar com o auxílio do conjunto de verificadores confiáveis previsto na diretriz 38 (“Aprimorar mecanismos de sinalização de conteúdo ilícito e de checagem de fatos na moderação de conteúdo”).

Trata-se de ações preventivas recomendadas especialmente nos casos em que há dúvida razoável sobre a ilicitude do conteúdo.

Diretriz 38

Aprimoramento de mecanismos de sinalização de conteúdo ilícito e de checagem de fatos na moderação de conteúdos

As plataformas de redes sociais devem adotar mecanismos eficazes para sinalização de conteúdo ilícito e para checagem na moderação de conteúdos. Recomenda-se, em especial, a adoção de processos e mecanismos para conferir tratamento prioritário a conteúdos ilícitos notificados por sinalizadores de confiança (*trusted flaggers*), isto é, um conjunto de entidades, públicas ou privadas, sem fins lucrativos e com atuação respeitada, conforme reconhecimento pela autoridade reguladora.

Outro mecanismo recomendado para ser incorporado na moderação de conteúdo é a adoção de ferramentas que promovam a checagem de fatos nas publicações de seus usuários para promover o acesso a infor-

mações de confiança. Por fim, podem ser estimulados mecanismos de moderação pela própria comunidade, como a adição de contexto pelos usuários, atentando-se aos riscos e características de cada plataforma de rede social.

Diretriz 11

Rotular o conteúdo sintético (gerado ou alterado significativamente por IA)

As plataformas de redes sociais devem promover a capacidade de rotular conteúdos sintéticos — isto é, aqueles gerados ou modificados significativamente por inteligência artificial —, de forma a dar transparência ao usuário sobre o conteúdo recebido. Elas devem ser estimuladas a identificar estes conteúdos sintéticos, de forma que a sua rotulagem não seja exclusivamente autodeclaratória (feita pelo produtor do conteúdo). É importante ainda que os respectivos autores do conteúdo e demais usuários tenham o direito de contestar a rotulagem e a forma como este é rotulado, isto é, os mecanismos, os processos e as decisões que resultam na identificação de um conteúdo como sintético.



Diretriz 39

Definir salvaguardas para o exercício da liberdade de expressão e devido processo na moderação de conteúdo

As plataformas de redes sociais devem prover ao usuário mecanismos ágeis de informação e contestação em caso de conteúdo removido ou perfil restrito. Os componentes do devido processo na moderação podem envolver elementos como transparência sobre a motivação da decisão, direito de solicitação de revisão, direito à revisão humana em caso de remoção automatizada e direito à reparação pela remoção indevida em caso de moderação revertida.

Da mesma forma, a regulação deve contemplar dispositivos para tornar as políticas de moderação protetivas ao exercício da liberdade de expressão

de seus usuários, especialmente para garantir o acesso à informação de qualidade.

Assim, esta diretriz pode contemplar também a implementação das seguintes espécies de moderação, igualmente sujeitas ao devido processo:

- “Moderação em camadas”, estabelecendo níveis de proteção a perfis que respeitam as regras da plataforma, mas que estão sujeitos a mais denúncias ou riscos de derrubada em razão de sua exposição, como os perfis de detentores de cargos políticos ou perfis de conteúdos jornalísticos;
- Redução de alcance (*down-ranking*) ou rotulagem de conteúdos como preferenciais em relação à remoção de conteúdo, que deve ser a última opção, considerando critérios como a gravidade do conteúdo.

**E EU, O QUE
POSSO FAZER?**



04

NESTA SEÇÃO, VOCÊ VAI ENCONTRAR:



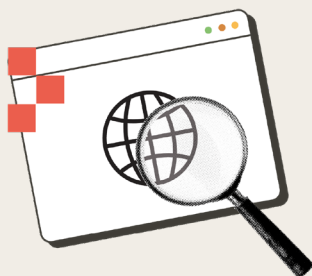
- Dicas de como se proteger e não propagar notícias falsas



1. Desconfie de títulos bombásticos

Uma prática comum de desinformação é a veiculação de títulos escandalosos e alarmistas que distorcem conteúdos antigos ou pouco relevantes. São os chamados “*clickbaits*” (“isca de clique”, em tradução livre), com a intenção de gerar o máximo possível de cliques, engajamento e visualizações motivados pela curiosidade^{103 104}.

Há alguns padrões recorrentes na construção desses títulos, como a construção textual incompleta, oferecendo pistas parciais para instigar a curiosidade; o modo imperativo (“acesse”, “entenda”, “veja”) para induzir o usuário a clicar; e o uso de exclamações, letras maiúsculas e superlativos, assim como promessas de “grandes revelações” que nem sempre condizem com o conteúdo apresentado.



2. Cuidado com conteúdos descontextualizados

➤ **Confira a data** da notícia e dos fatos. Às vezes, a notícia pode ser verdadeira, mas ocorreu em outro momento e está sendo usada fora de contexto¹⁰⁵.

➤ **Desconfie de afirmações categóricas.** Principalmente quando utilizam expressões como “sempre”, “nunca”, “todos”, “ninguém”, “não existe”, “nenhum governo”. Pesquisas recentes têm identificado, em conteúdos falsos, a presença maior de declarações formuladas de maneira categórica, sem nuances ou exceções¹⁰⁶.

➤ **Não confunda opinião com notícia.** Ainda que opiniões possam ser legítimas, as notícias se apoiam em fatos verificáveis, com base em fontes confiáveis e procedimentos adequados de apuração e checagem.

➤ Não confunda indícios com evidências.

Muitas vezes, determinados episódios ou casos concretos que possam ter chegado a você — ou a alguém que você conhece — podem não estar conectados entre si ou apontar para uma evidência mais ampla¹⁰⁷. Para que algo seja considerado evidência, deve se basear em um conjunto de métodos e procedimentos sistemáticos que contribuam para a verificação e a confiabilidade de determinada afirmação¹⁰⁸.

➤ Observe se há falhas visíveis.

Mesmo vídeos, imagens e capturas de imagens não são evidências em si sobre determinado fato e precisam de verificação. Com a evolução das *deepfakes*, esses materiais podem ser manipulados com alto grau de realismo e as falhas vêm sendo cada vez mais difíceis de identificar. Mas algumas inconsistências ainda são comuns:

No caso dos **áudios**, observe se a voz tem a emoção e a naturalidade condizentes com a pessoa e o assunto. Outros indícios possíveis são estalos, ruídos de fundo, cortes ou distorções que possam indicar edição.

No caso de **vídeos e fotos**, observe:

- » deformações em partes do corpo, como textura artificial nos cabelos e na pele, mais ou menos dedos nas mãos e desproporção entre o rosto e o corpo;
- » olhar estático, sem movimentos, ou incoerente com a interação da pessoa com as demais;
- » falhas na sincronia entre voz e imagem;
- » falta de fluidez nos movimentos corporais e na entonação da voz;
- » erros em elementos do cenário, como objetos deformados e palavras com a grafia errada¹⁰⁹.

Assistir vídeos no modo tela cheia facilita a percepção de adulterações¹¹⁰.

Por fim, um complemento indispensável é pesquisar pelo nome da pessoa que supostamente está falando ou pelos dizeres contidos no conteúdo e identificar notícias que desmintam ou confirmem as informações¹¹¹.



3. Pense antes de clicar

Seu clique é valiosíssimo para muitos agentes econômicos que atuam na Internet e que farão de tudo para chamar a sua atenção. Caso encontre uma informação interessante, mas que gere algum tipo de desconfiança (por exemplo, porque traz um dado muito urgente ou novo que não foi veiculado em nenhum outro lugar ainda), observe a fonte antes de clicar, pois algumas páginas podem ser criadas com o objetivo de obter dados específicos sobre você ou até mesmo atacar seu dispositivo. Mas preste atenção: muitas vezes, os *sites* criados para difundir conteúdos falsos possuem nomes muito parecidos com os de veículos de comunicação tradicionais¹¹².

4. Verifique as fontes

Uma forma de checar uma informação proveniente de uma fonte duvidosa é procurando a mesma informação no seu mecanismo de busca de preferência. Caso a informação seja verdadeira, você certamente a encontrará em veículos conhecidos, como *sites* oficiais, veículos de mídia reconhecidos e agências de checagem. Se for uma mentira, também é possível que você encontre relatos de outras pessoas questionando a veracidade da mesma notícia.

Um ponto de atenção importante é que, em 2026, influenciadores e perfis de fofocas com amplo número de seguidores têm contribuído para a disseminação de desinformação política¹¹³. Ainda que um perfil tenha amplo alcance, cabe avaliar se é o mais apropriado para oferecer aquele tipo de informação. É importante diferenciá-los de veículos jornalísticos que, em geral, submetem seus conteúdos a mecanismos de controle da qualidade da informação, que incluem padrões de apuração, checagem e confirmações das fontes.

Vale se perguntar: será que eu estou dando maior credibilidade do que aquela informação merece porque ela confirma as minhas crenças?

5. Desconfie de informações compartilhadas sem referências

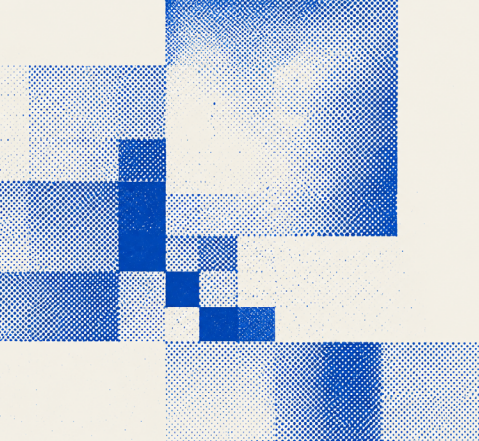
Quando receber alguma mensagem que não contenha referências (autor e data, por exemplo) ou fontes, pergunte à pessoa que a enviou como ela recebeu tal mensagem e como você pode verificar sua procedência. Outra opção é buscar *online* se há registros dessa informação em algum veículo de sua confiança — de preferência, fontes oficiais. O mesmo vale para fotos e vídeos, que podem ser compartilhados com títulos que os descontextualizem.

Lembre-se: mesmo pessoas próximas e confiáveis ou influenciadores de amplo alcance podem compartilhar informações erradas; esta é, aliás, uma das principais formas como a desinformação circula nas redes.



6. Na dúvida, não compartilhe

Nem sempre temos tempo de verificar tudo o que vemos ou recebemos; afinal, estamos expostos a uma quantidade imensa de informações diariamente. Nesse caso, a não ser que tenha plena confiança na fonte, não compartilhe uma informação sem verificar. Mesmo se enviada apenas para seu grupo fechado de familiares, ela pode causar estragos se alguém não romper com a corrente. Resista à tentação. Você terá outras oportunidades de analisar o conteúdo com mais calma e comentá-lo se quiser.



7. Não se cale: denuncie nos canais apropriados

Lembre-se de que muitas plataformas possuem canais nos quais você pode denunciar conteúdos que considere abusivos ou desinformativos e não hesite em utilizá-los caso se depare com esse tipo de material. Expressões de ódio são muito danosas à democracia e não são permitidas pelos termos de uso de várias redes sociais; é seu direito como usuário denunciar esse tipo de conteúdo. Além disso, caso você receba um conteúdo que saiba ser falso, avise a pessoa que o compartilhou e a oriente sobre os riscos desse tipo de material.

Como recomendação, o Tribunal Superior Eleitoral (TSE) disponibiliza dois canais principais:

SIADE: Sistema de Alertas de Desinformação Eleitoral

O Siade é um canal exclusivo para comunicar conteúdos falsos, enganosos ou descontextualizados que podem afetar a integridade das eleições. Os alertas são conferidos por uma equipe que analisa os casos e os comunica às plataformas digitais, para que elas avaliem se houve violação de suas regras. O Siade também enviará aos órgãos competentes os casos com indícios de crime ou infração administrativa eleitoral^{114 115}.

Como acessar?

<http://tse.jus.br/eleicoes/sistema-de-alertas>



Pardal: Ferramenta de Denúncias de Propaganda Eleitoral Irregular

Trata-se de uma ferramenta destinada ao recebimento de denúncias sobre infrações e irregularidades na propaganda eleitoral. A Justiça Eleitoral será responsável pela análise dos casos e pela adoção das medidas cabíveis.

Como acessar? Busque por “TSE Pardal” na loja de aplicativos do seu celular.



SAIBA MAIS



05

Saiba mais!

Reunimos algumas das referências utilizadas na produção deste guia e outras boas indicações para quem quer se aprofundar nos temas apresentados:

➤ **Enfrentando Deepfakes – Gustavo Souza e Tarcizio Silva (org.)**

<https://desvelar.org/enfrentando-deepfakes/>

➤ **Inteligência Artificial Generativa: Discriminação e Impactos Sociais – Tarcizio Silva (org.)**

https://acaoeducativa.org.br/wp-content/uploads/2024/11/Inteligencia-Artificial-Generativa-discriminacao-e-impactos-sociais_compressed.pdf

➤ **República do ódio: a dinâmica da extrema direita no WhatsApp, de José Maria da Silva do Rêgo Barreto e Pedro Jorge Chaves Mourão. Editora UFC, 2024.**

➤ **Radar Tecnológico: Inteligência Artificial Generativa – ANPD**

https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/radar_tecnologico_ia_generativa_anpd.pdf/@@display-file/file

➤ **Radar Tecnológico: Deepfakes – ANPD**

https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/rt_deepfakes_anpd.pdf/@@display-file/file

➤ **Anatomia da Desinformação Eleitoral – Agência Lupa**

https://uploads.agencialupa.org/2026/07/RELATORIO-ANATOMIA-DA-DESINFORMACAO-ELEITORAL_LUPA-FINAL.pdf

➤ **Sem Consentimento: Anúncios em redes sociais promovem falsos vídeos sexuais de Paolla Oliveira produzidos com inteligência artificial – Netlab UFRJ**

<https://netlab.eco.ufrj.br/post/sem-consentimento-an%C3%BAncios-em-redes-sociais-promovem-falsos-v%C3%ADdeos-sexuais-de-paolla-oliveira-produ>

- **Construindo Consensos: Deep Fakes nas Eleições de 2024 – Cedis: IDP**
<https://pos.idp.edu/blogs/producoes-cedis-inteligencia-artificial/construindo-consensos-deep-fakes-nas-eleicoes-de-2024-relatorio-das-decisoes-dos-tres-sobre-deep-fakes>
- **Painel TIC 2025: Pesquisa online com usuários de Internet no Brasil – Integridade da Informação – Cetic.br – NIC.br | CGI.br**
<https://cetic.br/pt/publicacao/painel-tic-2025-pesquisa-online-com-usuarios-de-internet-no-brasil-integridade-da-informacao/>
- **Caminhos da informação: Principais hábitos informacionais dos brasileiros por região – Aláfia Lab**
<https://alafialab.org/caminhos-da-informacao-principais-habitos-informacionais-dos-brasileiros-por-regiao/>
- **Boca de IA: Como as IAs recomendam voto nas eleições de 2026? – ITS Rio**
<https://itsrio.org/pt/publicacoes/boca-de-ia/>
- **Os Vetores da Comunicação política em aplicativos de mensagens: hábitos e percepções dos brasileiros – InternetLab**
https://internetlab.org.br/wp-content/uploads/2025/12/investigando-os-vetores-de-disseminacao-de-conteudo-eleitoral_Vfinal.pdf
- **Como os brasileiros percebem a circulação da desinformação e o uso da inteligência artificial – Aláfia Lab**
<https://alafialab.org/como-os-brasileiros-percebem-a-circulacao-da-desinformacao-e-o-uso-da-inteligencia-artificial/>
- **Guia Para influenciadores nas Eleições – InternetLab e Redes Cordiais**
<https://internetlab.org.br/pt/noticias/guia-para-influenciadores-orienta-sobre-regras-e-boas-praticas-para-atuacao-nas-eleicoes-de-2026/>
- **Cartilha “Boatos” – CERT.br – NIC.br | CGI.br**
<https://cartilha.cert.br/fasciculos/boatos/fasciculo-boatos.pdf>

Notas finais

- 1 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Princípios para a Regulação de Plataformas de Redes Sociais**. São Paulo: CGI.br, 2025. Disponível em: <https://cgi.br/pagina/principios-cgibr-regulacao-redes-sociais/>. Acesso em: 28 ago. 2026.
- 2 Trabalho decente, nos termos da Organização Internacional do Trabalho, é aquele adequadamente remunerado, exercido em condições de liberdade, equidade e segurança, capaz de garantir uma vida digna ao trabalhador.
- 3 ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Conselho de Direitos Humanos. **Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue**. Geneva: United Nations, 16 maio 2011. Documento A/HRC/17/27. Disponível em: <https://documents.un.org/doc/undoc/gen/g11/132/01/pdf/g1113201.pdf>. Acesso em: 18 ago. 2026,
- 4 CURZI, Yasmin. **Violência de Gênero Online**: regulação de plataformas e a proteção de direitos humanos de mulheres e pessoas de gênero dissidente no ambiente digital. Rio de Janeiro: Lumen Juris, 2026.
- 5 NEWMAN, Nic. **Overview and Key Findings of the 2016 Report**. Oxford: Reuters Institute for the Study of Journalism, 2016. Disponível em: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/archive/survey/2016/overview-key-findings-2016/index.html>. Acesso em: 18 ago. 2026.
- 6 NEWMAN, N. Executive summary and key findings of the 2020 report. **Reuters Institute Digital News Report**, 22 May 2020. Disponível em: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/archive/survey/2020/overview-key-findings-2020/index.html>. Acesso em: 18 ago. 2026.
- 7 EGAN, J. Overview and key findings of the 2026 Digital News Report. **Reuters Institute for the Study of Journalism**, 16 June 2026. Disponível em: <https://reutersinstitute.politics.ox.ac.uk/digital-news-report/2026/dnr-executive-summary>. Acesso em: 18 ago. 2026.
- 8 NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). **Painel TIC 2025**: pesquisa online com usuários de Internet no Brasil: integridade da informação. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2026. Disponível em: https://cetic.br/media/docs/publicacoes/2/pt-br/20260408150919/painel_tic_integridade_informacao_2026_livro_pt.pdf. PDF. Acesso em: 18 ago. 2026. p.23
- 9 Em 2025, 85% da população brasileira com 10 anos ou mais era usuária de Internet, percentual estável desde 2023. No entanto, 20% da população brasileira ainda se encontra no nível mais baixo de conectividade significativa, faixa que vem reduzindo gradualmente, mas ainda expressa desigualdades marcantes de classe social, escolaridade, cor ou raça, idade e território. Dados disponíveis em: NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). **Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros**: TIC Domicílios 2025. São Paulo: Comitê Gestor da Internet no Brasil, 2026.
- 10 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Guia Internet, democracia e eleições**. São Paulo: CGI.br, 2018. Disponível em: <https://cgi.br/publicacao/guia-internet-democracia-e-eleicoes/>. Acesso em: 8 set. 2026.
- 11 BBC BRASIL. Entenda o escândalo de uso político de dados que derrubou valor do FBBC

- NEWS BRASIL. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **BBC News Brasil**, 20 mar. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-43461751>. Acesso em: 21 set. 2026.
- 12 PERSILY, N.; TUCKER, J. A. Introduction. In: PERSILY, N.; TUCKER, J. A. (ed.). **Social media and democracy: the state of the field, prospects for reform**. Cambridge: Cambridge University Press, 2020. p. 1–9.
- 13 G1. ‘Pós-verdade’ é eleita a palavra do ano pelo Dicionário Oxford. **G1**, 16 nov. 2016. Disponível em: <https://g1.globo.com/educacao/noticia/pos-verdade-e-eleita-a-palavra-do-ano-pelo-dicionario-oxford.ghtml>. Acesso em: 14 set. 2026.
- 14 HAMM, L. **The few faces of disinformation**. EU DisinfoLab, 11 May 2020. Disponível em: <https://www.disinfo.eu/publications/the-few-faces-of-disinformation/>. Acesso em: 8 set. 2026.
- 15 WORLD HEALTH ORGANIZATION (WHO). **2019 Novel Coronavirus (2019-nCoV): strategic preparedness and response plan**. Geneva: WHO, 4 Feb. 2020. Disponível em: https://www.who.int/docs/default-source/coronaviruse/jmo-who-ncov-report-4feb-web.pdf?download=true&sfvrsn=d82d752a_2. PDF. Acesso em: 8 set. 2026.
- 16 WORLD HEALTH ORGANIZATION (WHO). **Director-General’s remarks at the media briefing on 2019 novel coronavirus on 8 February 2020**. Geneva: WHO, 8 Feb. 2020. Disponível em: <https://www.who.int/news-room/speeches/item/director-general-s-remarks-at-the-media-briefing-on-2019-novel-coronavirus---8-february-2020>. Acesso em: 8 set. 2026.
- 17 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br); NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). **Relatório Internet, Desinformação e Democracia**. São Paulo: CGI.br; NIC.br, 2020. Disponível em: <https://cgi.br/publicacao/relatorio-internet-desinformacao-e-democracia/>. Acesso em: 11 set. 2026.
- 18 BRADSHAW, S.; BAILEY, H.; HOWARD, P. N. **Industrialized disinformation: 2020 global inventory of organized social media manipulation**. Oxford: Programme on Democracy & Technology, 2021. 26 p. Disponível em: <https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/8/2021/02/CyberTroop-Report20-Draft9.pdf>. PDF. Acesso em: 8 set. 2026.
- 19 OBSERVATÓRIO LUPA. **Anatomia da desinformação eleitoral: como a mentira e os boatos políticos evoluíram no Brasil entre 2016 e 2026**. Rio de Janeiro: Lupa, 2026. Disponível em: https://uploads.agencialupa.org/2026/07/RELATORIO-ANATOMIA-DA-DESINFORMACAO-ELEITORAL_LUPA-FINAL.pdf. PDF. Acesso em: 18 ago. 2026.
- 20 OBSERVATÓRIO LUPA. **I Panorama da desinformação no Brasil: pessoas, entidades, plataformas e territórios afetados pelas mentiras digitais mais virais de 2025 e 2024**. Rio de Janeiro: Lupa, 2026. Disponível em: https://uploads.agencialupa.org/2026/02/Panorama_da_Desinformacao_no_Brasil_LUPA-1.pdf. PDF. Acesso em: 18 ago. 2026.
- 21 WORLD ECONOMIC FORUM. **The Global Risks Report 2025**. Geneva: World Economic Forum, 2025. Disponível em: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf. Acesso em: 21 set. 2026.
- 22 NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR (NIC.br). **Painel TIC 2025: pesquisa online com usuários de Internet no Brasil: integridade da informação**. 1. ed. São Paulo: Comitê Gestor da Internet no Brasil, 2026. Disponível em: https://www.cetic.br/media/docs/publicacoes/2/pt-br/20260408150919/painel_tic_integridade_

- informacao_2026_livro_pt.pdf. PDF. Acesso em: 8 set. 2026. p. 23
- 23 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Princípios para a Regulação de Plataformas de Redes Sociais**. São Paulo: CGI.br, 2025. Disponível em: <https://www.cgi.br/pagina/principios-cgibr-regulacao-redes-sociais/>. Acesso em: 8 set. 2026.
 - 24 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Princípios para a Regulação de Plataformas de Redes Sociais**. São Paulo: CGI.br, 2025. Disponível em: <https://www.cgi.br/pagina/principios-cgibr-regulacao-redes-sociais/>. Acesso em: 8 set. 2026.
 - 25 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Guia Internet, democracia e eleições**. São Paulo: CGI.br, 2018. Disponível em: <https://cgi.br/publicacao/guia-internet-democracia-e-eleicoes/>. Acesso em: 8 set. 2026.
 - 26 OBSERVATÓRIO LUPA. **I Panorama da desinformação no Brasil**: pessoas, entidades, plataformas e territórios afetados pelas mentiras digitais mais virais de 2025 e 2024. Rio de Janeiro: Lupa, 2026. Disponível em: https://uploads.agencialupa.org/2026/02/Panorama_da_Desinformacao_no_Brasil_LUPA-1.pdf. Acesso em: 18 ago. 2026.
 - 27 NAÇÕES UNIDAS. **Informe de política para a Nossa Agenda Comum**: integridade da informação nas plataformas digitais. Nova York: Nações Unidas, out. 2023. Disponível em: https://brasil.un.org/sites/default/files/2023-10/ONU_Integridade_Informacao_Plataformas_Digitais_Informe-Secretario-Geral_2023.pdf. Acesso em: 14 set. 2026.
 - 28 VIANA, N. No G20, Brasil pauta “integridade da informação” como princípio. **Agência Pública**. 7 maio 2024. Disponível em: <https://apublica.org/2024/05/no-g20-brasil-pauta-integridade-da-informacao-como-principio/>. Acesso em: 11 set. 2026.
 - 29 MENDONÇA, Y. C. de; ALMEIDA, C. L. de. Integridade da informação e responsabilidade de provedores de aplicação em relação à propaganda digital. **Revista Direito GV**, São Paulo, v. 22, e2622, 2026. DOI: <https://doi.org/10.1590/2317-6172202622>. Disponível em: https://www.scielo.br/jj/rdgv/a/pDrMc97gmZhh4phykpMVpzt/?format=html&lang=pt&ilang=pt_BR. Acesso em: 18 ago. 2026.
 - 30 SCHWARZ, O. **The Post-Choice Society**: Algorithmic Prediction and the Decentring of Choice. *Theory, Culture & Society*, [S. l.], v. 42, n. 4, p. 3–22, 2025. DOI: <https://doi.org/10.1177/02632764251322062>. Acesso em: 18 ago. 2026.
 - 31 WALKER, S. J. **Big Data**: A Revolution That Will Transform How We Live, Work, and Think. *International Journal of Advertising*, v. 33, n. 1, p. 181–183, 2014. DOI: <https://doi.org/10.2501/IJA-33-1-181-183>. Acesso em: 18 ago. 2026.
 - 32 SCHWARZ, O. **The Post-Choice Society**: Algorithmic Prediction and the Decentring of Choice. *Theory, Culture & Society*, v. 42, n. 4, p. 3–22, 2025. DOI: <https://doi.org/10.1177/02632764251322062>. Acesso em: 18 ago. 2026.
 - 33 KALIL, I. O. **Quem são e no que acreditam os eleitores de Jair Bolsonaro**. São Paulo: Fundação Escola de Sociologia e Política de São Paulo, 2018. Disponível em: <https://www.cartacapital.com.br/wp-content/uploads/2020/03/Relat%C3%B3rio-para-Site-FESPSP.pdf>. PDF. Acesso em: 18 ago. 2026.
 - 34 CESARINO, L. **Identidade e representação no bolsonarismo**: corpo digital do rei, bivalência conservadorismo-neoliberalismo e pessoa fractal. *Revista de Antropologia*, São Paulo, v. 62, n. 3, p. 530–557, 2019. DOI: <https://doi.org/10.11606/2179-0892.ra.2019.165232>. Disponível em: https://revistas.usp.br/ra/pt_BR/article/view/165232. Acesso em: 18 ago. 2016.

- 35 CURZI, Y. **Violência de gênero online:** regulação de plataformas e a proteção de direitos humanos de mulheres e pessoas de gênero dissidente no ambiente digital. Rio de Janeiro: Lumen Juris, 2026.
- 36 MENDONÇA, Y. C. de; ALMEIDA, C. L. de. Integridade da informação e responsabilidade de provedores de aplicação em relação à propaganda digital. **Revista Direito GV**, São Paulo, v. 22, e2622, 2026. DOI: <https://doi.org/10.1590/2317-6172202622>. Disponível em: https://www.scielo.br/jj/rdgv/a/pDrMc97gmZhh4phykpMVpzt/?format=html&lang=pt&ilang=pt_BR. Acesso em: 18 ago. 2026.
- 37 ANJOS, E. S. dos. IA e eleições de 2026: o desafio da soberania informacional. **Nexo Jornal**, 10 maio 2026. Disponível em: <https://www.nexojornal.com.br/ia-nas-eleicoes-presidenciais-2026-brasil-impacto-tecnologia>. Acesso em: 14 set. 2026.
- 38 WORLD ECONOMIC FORUM. **The Global Risks Report 2026**. 21st ed. Geneva: World Economic Forum, 2026. Disponível em: <https://www.weforum.org/publications/global-risks-report-2026/>. Acesso em: 10 set. 2026.
- 39 FERREIRA, L. C. IA acelera desinformação e ameaça democracias, alerta pesquisa. **Agência Brasil**, 16 abr. 2026. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2026-04/ia-acelera-desinformacao-e-ameaca-democracias-alerta-pesquisa>. Acesso em: 8 set. 2026.
- 40 BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital; SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO). **Guia de inteligência artificial generativa**. Brasília, DF: Ministério da Gestão e da Inovação em Serviços Públicos, [2025]. Disponível em: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/inteligencia-artificial-1/publicacoes/guia-ia-generativa>. Acesso em: 10 set. 2026.
- 41 VIEIRA, C. **Como os vieses entram na IA generativa?** In: SILVA, T. (org.). Inteligência artificial generativa: discriminação e impactos sociais. 2. ed. São Paulo: LiteraRUA, 2025. p. 19–26.
- 42 VIEIRA, C. **Como os vieses entram na IA generativa?** In: SILVA, T. (org.). Inteligência artificial generativa: discriminação e impactos sociais. 2. ed. São Paulo: LiteraRUA, 2025. p. 19–26.
- 43 AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Deepfakes**. Brasília, DF: ANPD, 2026. (Radar Tecnológico, n. 6). Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/rt_deepfakes_anpd.pdf. PDF. Acesso em: 10 set. 2026.
- 44 AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Deepfakes**. Brasília, DF: ANPD, 2026. (Radar Tecnológico, n. 6). Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/rt_deepfakes_anpd.pdf. PDF. Acesso em: 10 set. 2026.
- 45 NALON, T. Impacto da IA generativa nas eleições de 2024 é real, mas pode ser menor que o alardeado. **Aos Fatos**, [S. l.], 10 nov. 2023. Disponível em: <https://www.aosfatos.org/noticias/ia-generativa-impactos-eleicoes-2024/>. Acesso em: 11 set. 2026.
- 46 INTERNATIONAL PANEL ON THE INFORMATION ENVIRONMENT. **The role of generative AI use in 2024 elections worldwide**. Editado por I. Trauthig, P. N. Howard e S. Valenzuela. Zurich: IPIE, 2025. (Technical Paper, TP2025.2). DOI: <https://doi.org/10.61452/HZUE9853>.

- Disponível em: <https://www.ipie.info/research/tp2025-2>. Acesso em: 18 ago. 2026.
- 47 FIGUEIREDO, J. Campanha presidencial na Argentina usa inteligência artificial em grande escala. **O Globo**, Rio de Janeiro, 14 nov. 2023. Disponível em: <https://oglobo.globo.com/mundo/noticia/2023/11/14/campanha-presidencial-na-argentina-usa-ia-em-grande-escala.ghhtml>. Acesso em: 10 set. 2026.
- 48 ŁABUZ, M.; NEHRING, C. **On the way to deep fake democracy? Deep fakes in election campaigns in 2023**. *European Political Science*, v. 23, n. 4, p. 454–473, 2024. DOI: <https://doi.org/10.1057/s41304-024-00482-9>. Disponível em: <https://www.cambridge.org/core/journals/european-political-science/article/on-the-way-to-deep-fake-democracy-deep-fakes-in-election-campaigns-in-2023/8F97B6AD4C0B195B369696926B5F7EB>. Acesso em: 18 ago. 2026.
- 49 AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Deepfakes**. Brasília, DF: ANPD, 2026. (Radar Tecnológico, n. 6). Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-contenido/documentos-tecnicos-orientativos/rt_deepfakes_anpd.pdf. PDF. Acesso em: 10 set. 2026.
- 50 VIEIRA, A. L.; NASCIMENTO, K. ‘Ver pra crer’ morreu? De vídeo de Bolsonaro a avô morto pedindo voto, deepfakes entram nas campanhas; saiba identificar. **O Globo**, Rio de Janeiro, 4 set. 2026. Disponível em: <https://oglobo.globo.com/politica/eleicoes-2026/noticia/2026/09/04/ver-pra-crer-morreu-de-video-de-bolsonaro-a-avo-morto-pedindo-voto-deepfakes-entram-nas-campanhas-saiba-identificar.ghhtml>. Acesso em: 10 set. 2026.
- 51 CRUZ, I. Deepfake e edição: o fator vídeo na desinformação eleitoral. **Nexo Jornal**, São Paulo, 24 ago. 2022. Disponível em: <https://www.nexojornal.com.br/expresso/2022/08/24/deepfake-e-edicao-o-fator-video-na-desinformacao-eleitoral>. Acesso em: 10 set. 2026.
- 52 FERREIRA, L. C. IA acelera desinformação e ameaça democracias, alerta pesquisa. **Agência Brasil**, Brasília, DF, 16 abr. 2026. Disponível em: <https://agenciabrasil.ebc.com.br/geral/noticia/2026-04/ia-acelera-desinformacao-e-ameaca-democracias-alerta-pesquisa>. Acesso em: 10 set. 2026.
- 53 FALTAY, P. Como a IA reconfigura a ação política e por que é preciso definir regras rigorosas na disputa eleitoral. **Marco Zero Conteúdo**, [s. l.], 28 ago. 2026. Disponível em: <https://marcozero.org/como-a-ia-reconfigura-a-acao-politica-e-por-que-e-preciso-definir-regras-rigorosas-na-disputa-eleitoral/>. Acesso em: 10 set. 2026.
- 54 FARRUGIA, B. **Da urna ao algoritmo: lições de 2024 para enfrentar as deepfakes em 2026**. JOTA, [s. l.], 23 jul. 2025. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/da-urna-ao-algoritmo-lico-es-de-2024-para-enfrentar-as-deepfakes-em-2026>. Acesso em: 10 set. 2026.
- 55 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.732, de 27 de fevereiro de 2024**. Altera a Res.-TSE nº 23.610, de 18 de dezembro de 2019, dispondo sobre a propaganda eleitoral. Brasília, DF: Tribunal Superior Eleitoral, 2024. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>. Acesso em: 18 ago. 2026.
- 56 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.755, de 2 de março de 2026**. Altera a Resolução nº 23.610/TSE, de 18 de dezembro de 2019, que dispõe sobre propaganda eleitoral. Brasília, DF: Tribunal Superior Eleitoral, 2026. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2026/resolucao-no-23-755-de-2-de-marco-de-2026>. Acesso em: 10 set. 2026.

- 57 RODRIGUES, C.; NÓVOA, N.; MENDONÇA, E. IA nas eleições: as novas regras do TSE para propagandas eleitorais e plataformas. **Data Privacy Brasil Research**, [S. l.], 3 mar. 2026. Disponível em: <https://www.dataprivacybr.org/ia-nas-eleicoes-as-novas-regras-do-tse-para-propagandas-eleitorais-e-plataformas/>. Acesso em: 10 set. 2026.
- 58 VIEIRA, A. L.; NASCIMENTO, K. ‘Ver pra crer’ morreu? De vídeo de Bolsonaro a avô morto pedindo voto, deepfakes entram nas campanhas; saiba identificar. **O Globo**, Rio de Janeiro, 4 set. 2026. Disponível em: <https://oglobo.globo.com/politica/eleicoes-2026/noticia/2026/09/04/ver-pra-crer-morreu-de-video-de-bolsonaro-a-avo-morto-pedindo-voto-deepfakes-entram-nas-campanhas-saiba-identificar.ghtml>. Acesso em: 10 set. 2026.
- 59 CRUZ, I. Deepfake e edição: o fator vídeo na desinformação eleitoral. **Nexo Jornal**, São Paulo, 24 ago. 2022. Disponível em: <https://www.nexojornal.com.br/expresso/2022/08/24/deepfake-e-edicao-o-fator-video-na-desinformacao-eleitoral>. Acesso em: 10 set. 2026.
- 60 BATISTA PEREIRA, F. et al. **Fake news, fact checking, and partisanship**: the resilience of rumors in the 2018 Brazilian elections. *The Journal of Politics*, Chicago, v. 84, n. 4, p. 2188–2201, out. 2022. DOI: <https://doi.org/10.1086/719419>. Disponível em: <https://www.journals.uchicago.edu/doi/10.1086/719419>. Acesso em: 18 ago. 2026.
- 61 OROFINO, A. **A linguagem como ferramenta de transformação**. In: LAKOFF, G. Não pense num elefante: entenda seus valores e aprenda a enquadrar o debate. Tradução de Adriano Scandolara. São Paulo: Fósforo, 2026.
- 62 BATISTA PEREIRA, F. et al. **(De)mobilizing effects of misinformation**. SSRN Electronic Journal, 2025. DOI: <https://doi.org/10.2139/ssrn.5793363>. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5793363. Acesso em: 18 ago. 2026.
- 63 KARHAWI, I. **Influenciadores digitais**: conceitos e práticas em discussão. *Communicare*, São Paulo, v. 17, ed. esp., p. 46–61, 2017. Disponível em: <https://static.casperlibero.edu.br/uploads/2017/09/Artigo-1-Communicare-17-Edi%C3%A7%C3%A3o-Especial.pdf>. PDF. Acesso em: 18 ago. 2026.
- 64 INTERNETLAB; REDES CORDIAIS. **Guia para influenciadores nas eleições 2026**. 5. ed. [S. l.]: InternetLab; Redes Cordiais, 2026. Disponível em: https://internetlab.org.br/wp-content/uploads/2026/08/Guia_influenciadores_eleicoes_2026.pdf. PDF. Acesso em: 14 set. 2026.
- 65 DING, C.; JABR, W.; GUO, H. Electoral competition in the age of social media: the role of social media influencers. **MIS Quarterly**, v. 47, n. 4, p. 1647–1662, dez. 2023. DOI: <https://doi.org/10.25300/MISQ/2022/16422>. Acesso em: 18 ago. 2026.
- 66 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.610, de 18 de dezembro de 2019**. Dispõe sobre propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral. Brasília, DF: Tribunal Superior Eleitoral, 2019. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019>. Acesso em: 14 set. 2026.
- 67 ALVIM, F. F.; CARVALHO, V. O. A responsabilidade eleitoral dos influenciadores digitais pelo uso indevido dos meios de comunicação. **Revista Justiça Eleitoral em Debate**, Rio de Janeiro, v. 12, n. 1, p. 16–41, 2022. Disponível em: <https://revista.tre-rj.jus.br/rjed/article/view/149>. Acesso em: 18 ago. 2026.
- 68 CÓCOLO, V. Brasil tem 18 ‘Donas Marias’, e a maioria delas não informa que é IA. **G1**, 20 maio 2026. Disponível em: <https://g1.globo.com/politica/eleicoes/2026/>

- noticia/2026/05/20/maioria-dos-avatars-politicos-criados-por-ia-nas-redes-nao-informa-
uso-da-tecnologia-diz-estudo.ghtml. Acesso em: 10 set. 2026.
- 69 TOLEDO, L. F. A personagem de IA que viraliza com críticas ao governo Lula e ao STF. **BBC News Brasil**, 14 abr. 2026. Disponível em: <https://www.bbc.com/portuguese/articles/c7vq10lvv15o>. Acesso em: 10 set. 2026.
 - 70 TOLEDO, L. F. A personagem de IA que viraliza com críticas ao governo Lula e ao STF. **BBC News Brasil**, 14 abr. 2026. Disponível em: <https://www.bbc.com/portuguese/articles/c7vq10lvv15o>. Acesso em: 10 set. 2026.
 - 71 ROMEU, A. Eleições presidenciais no Brasil: medidas contra a desinformação eleitoral online são amplamente insuficientes. **Repórteres Sem Fronteiras**, [S. l.], 16 set. 2026. Disponível em: <https://rsf.org/pt-br/elei%C3%A7%C3%B5es-presidenciais-no-brasil-medidas-contra-desinforma%C3%A7%C3%A3o-eleitoral-online-s%C3%A3o-amplamente>. Acesso em: 21 set. 2026.
 - 72 BERTHIER, V. Cem deepfakes analisados: RSF alerta para uma ameaça crescente aos jornalistas, especialmente às mulheres. **Repórteres Sem Fronteiras**, [S. l.], 4 fev. 2026. Disponível em: <https://rsf.org/pt-br/cem-deepfakes-analisados-rsf-alerta-para-uma-amea%C3%A7a-crescente-aos-jornalistas-especialmente-%C3%A0s>. Acesso em: 21 set. 2026.
 - 73 FALTAY, P. Como a IA reconfigura a ação política e por que é preciso definir regras rigorosas na disputa eleitoral. **Marco Zero Conteúdo**, [S. l.], 28 ago. 2026. Disponível em: <https://marcozero.org/como-a-ia-reconfigura-a-acao-politica-e-por-que-e-preciso-definir-regras-rigorosas-na-disputa-eleitoral/>. Acesso em: 10 set. 2026.
 - 74 GAMA, R. Da Dona Maria ao Zé da Feira, ‘fakes sintéticos’ inundam as redes e driblam TSE com narrativas pró e contra governo. **O Globo**, Rio de Janeiro, 5 maio 2026. Disponível em: <https://oglobo.globo.com/blogs/sonar-a-escuta-das-redes/post/2026/05/da-dona-maria-ao-ze-da-feira-fakes-sinteticos-inundam-as-redes-e-driblam-tse-com-narrativas-pro-e-contra-governo.ghtml>. Acesso em: 10 set. 2026.
 - 75 FALTAY, P. Como a IA reconfigura a ação política e por que é preciso definir regras rigorosas na disputa eleitoral. **Marco Zero Conteúdo**, [S. l.], 28 ago. 2026. Disponível em: <https://marcozero.org/como-a-ia-reconfigura-a-acao-politica-e-por-que-e-preciso-definir-regras-rigorosas-na-disputa-eleitoral/>. Acesso em: 10 set. 2026.
 - 76 FALTAY, P. Como a IA reconfigura a ação política e por que é preciso definir regras rigorosas na disputa eleitoral. **Marco Zero Conteúdo**, [S. l.], 28 ago. 2026. Disponível em: <https://marcozero.org/como-a-ia-reconfigura-a-acao-politica-e-por-que-e-preciso-definir-regras-rigorosas-na-disputa-eleitoral/>. Acesso em: 10 set. 2026.
 - 77 AJDER, H. et al. **The state of deepfakes: landscape, threats, and impact**. [S. l.]: Deeptrace Labs, 2019. Disponível em: <https://docslib.org/doc/12559428/the-state-of-deepfakes-landscape-threats-and-impact-henry-ajder-giorgio-patrini-francesco-cavalli-and-laurence-cullen-september-2019>. Acesso em: 18 ago. 2026.
 - 78 SECURITY HERO. **State of deepfakes: realities, threats, and impact**. [S. l.]: Security Hero, 2023. Disponível em: <https://www.securityhero.io/state-of-deepfakes/>. Acesso em: 10 set. 2026.
 - 79 HAWKINS, W.; RUSSELL, C.; MITTELSTADT, B. **Deepfakes on demand: the rise of accessible non-consensual deepfake image generators**. In: ACM CONFERENCE ON

- FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY, 2025, Athens. Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency. New York: Association for Computing Machinery, 2025. p. 1602–1614. DOI: <https://doi.org/10.1145/3715275.3732107>. Acesso em: 18 ago. 2026.
- 80 N WOMEN. **Tipping point**: the chilling escalation of online violence against women in the public sphere. New York: UN Women, dez. 2025. Disponível em: <https://openaccess.city.ac.uk/id/eprint/37570/1/tipping-point-the-chilling-escalation-of-violence-against-women-in-the-public-sphere-in-the-age-of-ai-en.pdf>. PDF. Acesso em: 10 set. 2026.
- 81 DING, M. L.; SURESH, H.; VENKATASUBRAMANIAN, S. How to stop playing whack-a-mole: mapping the ecosystem of technologies facilitating AI-generated non-consensual intimate images. **arXiv**, 2026. DOI: <https://doi.org/10.48550/arXiv.2602.04759>. Disponível em: <https://arxiv.org/abs/2602.04759>. Acesso em: 16 ago. 2026.
- 82 INTERNETLAB; REVISTA AZMINA; NÚCLEO JORNALISMO; LABHD-UFBA. **MonitorA**: relatório sobre violência política contra candidatas(os) online: edição 2024. São Paulo: InternetLab; Revista AzMina; Núcleo Jornalismo; LABHD-UFBA, 2025. Disponível em: https://internetlab.org.br/wp-content/uploads/2025/05/MonitorA-Relatorio_2024-3.pdf. PDF.
- 83 MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS (MPDFT). Deepfakes nas eleições abrem nova frente de atenção à violência política de gênero. **MPDFT**, Brasília, DF, 1 set. 2026. Disponível em: <https://www.mpdft.mp.br/portal/index.php/comunicacao-menu/sala-de-imprensa/noticias/noticias-2026/18173-deepfakes-nas-eleicoes-abrem-nova-frente-de-atencao-a-violencia-politica-de-genero>. Acesso em: 10 set. 2026.
- 84 INTERNETLAB; REVISTA AZMINA; NÚCLEO JORNALISMO; LABHD-UFBA. **MonitorA**: relatório sobre violência política contra candidatas(os) online: edição 2024. São Paulo: InternetLab; Revista AzMina; Núcleo Jornalismo; LABHD-UFBA, 2025. Disponível em: https://internetlab.org.br/wp-content/uploads/2025/05/MonitorA-Relatorio_2024-3.pdf. PDF.
- 85 INSTITUTO MARIELLE FRANCO. **Regime de ameaça**: a violência política de gênero e raça no âmbito digital. Rio de Janeiro: Instituto Marielle Franco, 2025. Disponível em: <https://www.violenciapolitica.org/>. PDF. Acesso em: 15 jun. 2026.
- 86 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Nota pública sobre exploração sexual por uso indevido de inteligência artificial generativa**. São Paulo: CGI.br, 2025. Disponível em: <https://cgi.br/esclarecimentos/ver/nota-publica-sobre-exploracao-sexual-por-uso-indevido-de-inteligencia-artificial-generativa.pdf>. PDF. Acesso em: 10 set. 2026.
- 87 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Nota técnica do CGI.br sobre o PL 2.338/2023**: regulação da inteligência artificial no Brasil. São Paulo: CGI.br, 2026. Disponível em: <https://cgi.br/publicacao/nota-tecnica-do-cgi-br-sobre-o-pl-2-338-2023-regulacao-da-inteligencia-artificial-no-brasil/>. Acesso em: 18 ago. 2026.
- 88 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Nota técnica do CGI.br sobre violência de gênero em ambientes digitais**. São Paulo: CGI.br, 2026. Disponível em: <https://cgi.br/publicacao/nota-tecnica-do-cgi-br-sobre-violencia-de-genero-em-ambientes-digitais/>. Acesso em: 18 ago. 2026.
- 89 PROJETO BRIEF. IA e eleições 2026. [S. l.]: **Projeto Brief**, 2026. Disponível em: <https://www.projetobrief.com/especiais/ia-eleicoes-2026>. Acesso em: 10 set. 2026.

- 90 INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO DE JANEIRO (ITS RIO). **Boca de IA:** como as IAs recomendam voto nas eleições de 2026? Rio de Janeiro: ITS Rio, 2026. Disponível em: <https://itsrio.org/wp-content/uploads/2017/01/Boca-de-IA.pdf>. PDF. Acesso em: 10 set. 2026.
- 91 DANTAS, G. Textos gerados por inteligência artificial convencem mais do que deepfakes, aponta relatório. **Desinformante**, 8 jul. 2026. Disponível em: <https://desinformante.com.br/texto-ia-deepfake-pesquisa/>. Acesso em: 10 set. 2026.
- 92 YUAN, H. et al. The cultural stereotype and cultural bias of ChatGPT. **Journal of Pacific Rim Psychology**, v. 19, art. 18344909251355673, 2025. DOI: <https://doi.org/10.1177/18344909251355673>.
- 93 STOKEL-WALKER, C. **ChatGPT replicates gender bias in recommendation letters**. Scientific American, 22 nov. 2023. Disponível em: <https://www.scientificamerican.com/article/chatgpt-replicates-gender-bias-in-recommendation-letters/>. Acesso em: 18 ago. 2026.
- 94 HOFMANN, V. et al. AI generates covertly racist decisions about people based on their dialect. **Nature**, v. 633, p. 147–154, 2024. DOI: <https://doi.org/10.1038/s41586-024-07856-5>.
- 95 LIU, R. et al. Quantifying and alleviating political bias in language models. **Artificial Intelligence**, v. 304, art. 103654, 2022. DOI: <https://doi.org/10.1016/j.artint.2021.103654>. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0004370221002058>. Acesso em: 10 set. 2026.
- 96 KOZLOV, M. AI chatbots can sway voters with remarkable ease — is it time to worry? **Nature**, 4 dez. 2025. Disponível em: <https://www.nature.com/articles/d41586-025-03975-9>. Acesso em: 10 set. 2026.
- 97 SIMMS, C. AI is more persuasive than people in online debates. **Nature**, 19 maio 2025. Disponível em: <https://www.nature.com/articles/d41586-025-01599-7>. Acesso em: 10 set. 2026.
- 98 MCGUFFIE, K.; NEWHOUSE, A. The radicalization risks of GPT-3 and advanced neural language models. **arXiv**, arXiv:2009.06807, 2020. DOI: <https://doi.org/10.48550/arXiv.2009.06807>. Disponível em: <https://arxiv.org/abs/2009.06807>. Acesso em: 10 set. 2026.
- 99 BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.755, de 2 de março de 2026**. Altera a Resolução-TSE nº 23.610, de 18 de dezembro de 2019, que dispõe sobre propaganda eleitoral. Brasília, DF: Tribunal Superior Eleitoral, 2026. Disponível em: <https://www.tse.jus.br/legislacao/compilada/res/2026/resolucao-no-23-755-de-2-de-marco-de-2026>. Acesso em: 18 ago. 2026.
- 100 INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO DE JANEIRO (ITS RIO). **Boca de IA:** como as IAs recomendam voto nas eleições de 2026? Rio de Janeiro: ITS Rio, 2026. Disponível em: <https://itsrio.org/wp-content/uploads/2017/01/Boca-de-IA.pdf>. PDF. Acesso em: 10 set. 2026.
- 101 As diretrizes que constam neste documento são uma versão adaptada das Diretrizes Para Regulação de Plataformas de Redes Sociais, publicadas em setembro de 2026 pelo CGI. br. Respectivamente, são as diretrizes de número: 4, 10, 32, 33, 7, 36, 38, 11 e 6. Acesse na

íntegra: <https://cgi.br/pagina/diretrizes-plataformas/>

- 102 Critérios considerados pelos algoritmos para recomendação de conteúdo a um determinado usuário, entre os quais localização, idade, gênero e publicações curtidas. COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Diretrizes para regulação de plataformas de redes sociais**. Resolução CGI.br/RES/2026/082, de 21 de agosto de 2026. São Paulo: CGI.br, 2026. Disponível em: <https://www.cgi.br/resolucoes/documento/2026/082/>. Acesso em: 30 set. 2026.
- 103 SENADO VERIFICA. Clickbait: descubra como títulos exagerados podem enganar você. **Senado Verifica**, Brasília, DF, 20 jun. 2026. Disponível em: <https://www12.senado.leg.br/verifica/materias-especiais/2026/clickbait-descubra-como-titulos-exagerados-podem-enganar-voce>. Acesso em: 11 set. 2026.
- 104 CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Boatos**. São Paulo: NIC.br, jul. 2024. (Cartilha de Segurança para Internet. Fascículos). Disponível em: <https://cartilha.cert.br/fasciculos/boatos/fasciculo-boatos.pdf>. PDF. Acesso em: 11 set. 2026.
- 105 CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Boatos**. São Paulo: NIC.br, jul. 2024. (Cartilha de Segurança para Internet. Fascículos). Disponível em: <https://cartilha.cert.br/fasciculos/boatos/fasciculo-boatos.pdf>. PDF. Acesso em: 11 set. 2026.
- 106 OBSERVATÓRIO LUPA. **Anatomia da desinformação eleitoral**: como a mentira e os boatos políticos evoluíram no Brasil entre 2016 e 2026. Rio de Janeiro: Lupa, 2026. Disponível em: https://uploads.agencialupa.org/2026/07/RELATORIO-ANATOMIA-DA-DESINFORMACAO-ELEITORAL_LUPA-FINAL.pdf. PDF. Acesso em: 18 ago. 2026.
- 107 DEMURU, Paolo. **Políticas do Encanto**. P. 29. São Paulo: Elefante, 2024. DEMURU, P. Políticas do encanto: extrema direita e fantasias da conspiração. São Paulo: Elefante, 2024. p. 29.
- 108 Na literatura científica, há dezenas de conceitos de “evidência”, que podem variar, também, a depender do campo de conhecimento, como nas ciências sociais, da saúde e no campo jurídico. Para os fins da discussão aqui proposta, partimos de elementos em comum encontrados em diversas definições de “evidência” em revisão de literatura sobre o tema. YU, X. et al. Exploring the diverse definitions of ‘evidence’: a scoping review. **BMJ Evidence-Based Medicine**, v. 29, n. 1, p. 37–43, 2024. DOI: <https://doi.org/10.1136/bmjebm-2023-112355>. Disponível em: <https://ebm.bmj.com/content/29/1/37>. Acesso em: 11 set. 2026.
- 109 SOUZA, M. Como identificar conteúdos falsos sobre saúde nas redes sociais. **Nexo Jornal**, 3 set. 2026. Disponível em: <https://www.nexojornal.com.br/servico/2026/09/03/saude-desinformacao-como-identificar-noticia-falsa>. Acesso em: 11 set. 2026.
- 110 CRUZ, I. Deepfake e edição: o fator vídeo na desinformação eleitoral. **Nexo Jornal**, 24 ago. 2022. Disponível em: <https://www.nexojornal.com.br/expresso/2022/08/24/deepfake-e-edicao-o-fator-video-na-desinformacao-eleitoral>. Acesso em: 11 set. 2026.
- 111 CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL (CERT.br). **Boatos**. São Paulo: NIC.br, jul. 2024. (Cartilha de Segurança para Internet. Fascículos). Disponível em: <https://cartilha.cert.br/fasciculos/boatos/fasciculo-boatos.pdf>. PDF. Acesso em: 11 set. 2026.

- 112 COMITÊ GESTOR DA INTERNET NO BRASIL (CGI.br). **Guia Internet, democracia e eleições**. São Paulo: CGI.br, 2018. Disponível em: <https://cgi.br/publicacao/guia-internet-democracia-e-eleicoes/>. Acesso em: 18 ago. 2026.
- 113 COELHO, L. **Quando as fofocas se tornam mensagens políticas**. LatAm Journalism Review, 4 fev. 2026. Disponível em: <https://latamjournalismreview.org/pt-br/articles/quando-as-fofocas-se-tornam-mensagens-politicas/>. Acesso em: 11 set. 2026.
- 114 BRASIL. Tribunal Superior Eleitoral. **Sistema de Alertas de Desinformação Eleitoral (SIADÉ)**. Brasília, DF: Tribunal Superior Eleitoral, [s. d.]. Disponível em: <https://www.tse.jus.br/eleicoes/sistema-de-alertas>. Acesso em: 11 set. 2026.
- 115 Para dicas de como usar cada um dos canais recomendados, veja passo a passo em: DANTAS, G. Como denunciar desinformação nas eleições: veja o passo a passo nos canais oficiais do TSE. **Desinformante**, 19 ago. 2026. Disponível em: <https://desinformante.com.br/como-denunciar-desinformacao-tse/>. Acesso em: 11 set. 2026.

