XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

GUSTAVO RABAY GUERRA

JOSÉ RENATO GAZIERO CELLA

JÉSSICA FACHIN

I61

Internet: dinâmicas da segurança pública internacional[Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto, Gustavo Rabay Guerra, José Renato Gaziero Cella, Jéssica Fachin – Florianópolis: CONPEDI, 2025.

Inclui bibliografia
ISBN: 978-65-5274-285-8
Modo de acesso: www.conpedi.org.br em publicações
Tema: Os Caminhos Da Internacionalização E O Futuro Do Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. XXXII Congresso Nacional do CONPEDI São Paulo - SP (4: 2025: Florianópolis, Brasil).

CDU: 34

XXXII CONGRESSO NACIONAL DO CONPEDI SÃO PAULO - SP

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

No XXII Congresso Nacional do CONPEDI, realizado nos dias 26, 27 e 28 de novembro de 2025, o Grupo de Trabalho - GT “Internet: Dinâmicas da Segurança Pública e Internacional”, que teve lugar na tarde de 28 de novembro de 2025, destacou-se no evento não apenas pela qualidade dos trabalhos apresentados, mas pelos autores dos artigos, que são professores pesquisadores acompanhados de seus alunos pós-graduandos. Foram apresentados artigos objeto de um intenso debate presidido pelos coordenadores.

Esse fato demonstra a inquietude que os temas debatidos despertam na seara jurídica. Cientes desse fato, os programas de pós-graduação em direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao direito. Para apresentar e discutir os trabalhos produzidos sob essa perspectiva.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “Internet: Dinâmicas da Segurança Pública e Internacional”. Trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em direito, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores

Prof. Dr. José Renato Gaziero Cella

Prof. Dra. Danielle Jacon Ayres Pinto

Prof. Dr. Gustavo Rabay Guerra

Prof. Dra. Jéssica Fachin

DESINFORMAÇÃO NA ERA DA INTELIGÊNCIA ARTIFICIAL E SEUS IMPACTOS NA SEGURANÇA INTERNACIONAL: UM ESTUDO DE CASO SOBRE O BRASIL

DISINFORMATION IN THE AGE OF ARTIFICIAL INTELLIGENCE AND ITS IMPACTS ON INTERNATIONAL SECURITY: A BRAZILIAN CASE STUDY

Maria Amélia Carvalho Campos [1]
Thayane Brito de Jesus [2]

Resumo

Este artigo investiga a relação entre inteligência artificial, desinformação e segurança internacional, focando na ausência de uma regulação específica no Brasil. O problema central busca compreender como esse vácuo normativo impacta a segurança do país frente às estratégias de guerra híbrida informacional. A pesquisa parte da hipótese de que a carência de leis amplia a vulnerabilidade brasileira a ataques de desinformação, em comparação com blocos regulatórios mais consolidados, como a União Europeia. Utilizando uma abordagem hipotético-dedutiva com revisão bibliográfica, a pesquisa analisa desde o modelo da economia da atenção, que fomenta a desinformação, até os impactos dos deepfakes gerados por IA na autenticidade dos fatos. A investigação confirma a hipótese, concluindo que a falta de leis torna o Brasil um alvo suscetível à manipulação e desestabilização democrática. O fracasso do PL 2.630/2020 é apontado como uma estratégia regulatória equivocada que resultou no atual despreparo legal. Por fim, sugere-se uma mudança de paradigma: abandonar a regulação ampla de plataformas e adotar uma abordagem segmentada, focada em regular atividades digitais danosas, a fim de construir uma defesa jurídica mais eficaz para a democracia na era da guerra informacional.

Palavras-chave: Desinformação, Inteligência artificial, Guerra híbrida, Regulação de plataformas, Segurança internacional

Abstract/Resumen/Résumé

This paper investigates the relationship between artificial intelligence, disinformation, and international security, focusing on the absence of specific regulation in Brazil. The central problem seeks to understand how this normative vacuum impacts the country's security in the face of informational hybrid warfare strategies. The research is based on the hypothesis that the lack of laws increases Brazil's vulnerability to disinformation attacks, compared to more consolidated regulatory blocs such as the European Union. Using a hypothetical-deductive

[1] Advogada, Mestranda em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie (UPM), em associação com a Universidade Federal de Mato Grosso do Sul (UFMS); e-mail: amelia.campos@ufms.br.

[2] Advogada e Mestranda em Direito Político e Econômico pela Universidade Presbiteriana Mackenzie (UPM), em associação com a Universidade Federal de Mato Grosso do Sul (UFMS). Técnica de Nível Superior da Universidade Estadual de Mato Grosso do Sul (UEMS). E-mail: thayanebrito@outlook.com

approach with a literature review, the research analyzes everything from the attention economy model, which fosters disinformation, to the impacts of AI-generated deepfakes on the authenticity of facts. The investigation confirms the hypothesis, concluding that the lack of laws makes Brazil a susceptible target for manipulation and democratic destabilization. The failure of Bill 2,630/2020 is pointed out as a misguided regulatory strategy that resulted in the current legal unpreparedness. Finally, a paradigm shift is suggested: abandoning broad platform regulation and adopting a segmented approach focused on regulating harmful digital activities, in order to build a more effective legal defense for democracy in the age of informational warfare.

Keywords/Palabras-claves/Mots-clés: Disinformation, Artificial intelligence, Hybrid warfare, Platform regulation, International security

1. INTRODUÇÃO

O avanço tecnológico nas últimas décadas transformou a forma como informações são produzidas, distribuídas e consumidas. A internet, concebida originalmente como um espaço de compartilhamento gratuito de bens imateriais, evoluiu para um ambiente em que plataformas digitais monetizam a atenção dos usuários por meio de modelos baseados na publicidade. Consequentemente, o modelo da "economia da atenção" criou condições propícias para a disseminação de desinformação, ao privilegiar conteúdos que provocam forte engajamento, independentemente de sua veracidade.

Nesse contexto, destaca-se o avanço recente das ferramentas de inteligência artificial (IA), especialmente em suas aplicações generativas, e os *deepfakes* emergem como instrumentos poderosos capazes de manipular percepções, distorcer a realidade e influenciar decisões políticas e sociais.

No Brasil, a regulação específica sobre inteligência artificial e plataformas digitais ainda é incipiente, o que levanta questionamentos sobre a vulnerabilidade do país diante do uso de estratégias de guerra híbrida informacional. Nesse contexto, surgem dúvidas sobre como *fake news* e conteúdos manipulados, como *deepfakes*, podem ser utilizados como instrumentos de influência política e geopolítica.

Além disso, observa-se a necessidade de investigar como a ausência de regulamentação se compara a experiências internacionais, como a União Europeia, que busca estabelecer normas sobre a atuação de plataformas digitais e a proteção da integridade das informações e dos direitos fundamentais.

Dessa forma, a relevância desta pesquisa se manifesta em duas dimensões. No campo jurídico, destaca-se a pertinência de investigar a existência ou não de lacunas normativas relacionadas ao uso de inteligência artificial, à proteção de dados e à responsabilidade das plataformas digitais diante da propagação de desinformação.

No campo científico, a pesquisa busca aprofundar a compreensão das interações entre tecnologia, segurança internacional e estratégias de guerra híbrida, com atenção especial ao modo como diferentes cenários regulatórios podem influenciar a posição do Brasil em contextos geopolíticos e de disputas internacionais.

A partir disso, apresenta-se o problema de pesquisa que orienta este estudo: de que maneira a ausência de regulação da inteligência artificial e das plataformas digitais no Brasil impacta a segurança internacional diante da disseminação de desinformação?

Diante disso, a presente investigação, de abordagem hipotético-dedutiva, parte da hipótese de que a ausência de regulação específica sobre inteligência artificial e plataformas digitais no Brasil amplia a vulnerabilidade do país frente às estratégias de guerra híbrida informacional, tornando-o mais exposto a *fake news* e *deepfakes* em comparação a blocos regulatórios mais consolidados, como a União Europeia.

Para tanto, a pesquisa se apoia em revisão bibliográfica sobre desinformação, segurança internacional e inteligência artificial, além de estudo de casos que analisam episódios de uso de desinformação em estratégias de guerra híbrida. Desse modo, este estudo tem como objetivo central compreender e investigar a relação entre inteligência artificial, *fake news* e segurança internacional, considerando a ausência de regulação no Brasil.

Nesse ínterim, os objetivos específicos incluem: discutir a centralidade do modelo da economia da atenção na propagação de desinformação; analisar os impactos da IA generativa e dos *deepfakes* sobre a autenticidade das informações; identificar vulnerabilidades específicas do Brasil diante da falta de regulação; e examinar a experiência regulatória da União Europeia, por meio do *Digital Services Act*, para compreender possíveis lições aplicáveis ao contexto brasileiro.

2. A ECONOMIA DA ATENÇÃO E A PROPAGAÇÃO DA DESINFORMAÇÃO

Ao longo das últimas décadas, a economia global passou por transformações profundas, impulsionadas pelo avanço das tecnologias digitais e pela emergência das plataformas online. As empresas deixaram de operar apenas em mercados físicos ou tradicionais, passando a explorar novas formas de interação com consumidores e fornecedores, baseadas em dados e algoritmos.

Nesse sentido, a inovação central das plataformas digitais não reside apenas na automação ou na conectividade, mas na forma como estas conseguem moldar e personalizar seus serviços conforme o perfil e o comportamento dos usuários, conforme aponta Bachur:

> O momento decisivo em que as plataformas digitais transformaram a economia mundial de fins do século XX e início do XXI está em associar uma determinada atividade empresarial à personalização dessa atividade. (BACHUR, 2021, p. 448)

A mudança na lógica publicitária foi decisiva para a consolidação do modelo de negócios atualmente utilizado pelas plataformas de redes sociais. O núcleo do poder e da

complexidade das plataformas passou a residir em um modelo de negócio que não se baseia na cobrança pelo serviço, mas na monetização da atenção do usuário.

Com a decaída da efetividade do marketing tradicional e o surgimento de uma estratégia mais barata, os anunciantes reformularam seu modelo de negócio. Desse modo, as plataformas trocam o acesso "gratuito" por dados, que são processados por *Big Data* para criar perfis de usuário microsegmentados.

Essa atenção segmentada é vendida à anunciantes com uma taxa de conversão drasticamente superior à da mídia tradicional, gerando um ciclo de engajamento e receita que incentiva a amplificação de conteúdos, independentemente de sua veracidade ou qualidade. Assim, os perfis se tornam "micromundos", onde o conteúdo exibido é perfeitamente ajustado para agradar o indivíduo, tornando o espaço digital mais confortável e adequado aos seus gostos.

Desse modo, por meio de algoritmos que buscam inferir os desejos dos usuários antes mesmo que eles os expressem conscientemente, explorando vieses e gatilhos emocionais, as plataformas retêm a permanência do usuário, aumentando o tempo de atividade e lucrando com a venda da atenção desses usuários à anunciantes.

> As grandes empresas de tecnologia são, antes de tudo, *empresas*: organizações comerciais que, para maximizar seus rendimentos, precisam encorajar os usuários a permanecerem *on-line* o maior tempo possível, ampliando a exposição ao *marketing* (Wardle; Derakhshan, 2017, p. 52). Isso é feito com base no engajamento pretérito do usuário (curtidas, comentá- rios, compartilhamentos etc.). Por isso a dimensão temporal é importante: tanto em relação ao tempo que cada usuário gasta interagindo nas novas mídias digitais quanto em relação ao tempo que as plataformas tiveram para acumular dados pessoais de seus usuários. Para as plataformas, o ideal é que todos gastem o maior tempo possível *on-line*. (BACHUR, 2021, p. 451)

De modo geral, o ambiente digital transformou a atenção do usuário em uma mercadoria e remodelou a esfera pública em torno do engajamento em vez da credibilidade. Nesse contexto, o valor de uma informação deixou de depender de sua veracidade ou relevância social e passou a ser medido pela capacidade de gerar interação: curtidas, comentários e compartilhamentos se tornaram métricas de prestígio e visibilidade. Esse fenômeno revela como, nas plataformas digitais, o critério de sucesso de um conteúdo não é mais a correspondência aos fatos, mas sim a circulação que consegue alcançar.

> O critério crucial de valorização de conteúdos nas plataformas algorítmicas é a circulação: os conteúdos que se impõem são aqueles que granjeiam maior repercussão. Ou seja, a verdade é aquela estatisticamente contingente, não a ontologicamente essencial, definida pela correspondência aos fatos. (CASTRO, 2019, p. 13)

A lógica de valorização do conteúdo pela circulação apresenta relação direta com a velocidade com que a informação se propaga no ambiente digital. O dinamismo inerente às plataformas digitais faz com que a informação circule praticamente de forma instantânea, o que amplia o alcance do conhecimento, mas simultaneamente potencializa seus efeitos negativos, pois a pressão por atualização constante pode se sobrepor à análise crítica e fundamentada do conteúdo que é recebido pelo usuário.

> A digitalização aplicada à comunicação tornou possível que as informações circulem pelo mundo praticamente em tempo real. Embora seja certo que isso abra possibilidades ilimitadas para a transmissão e ampliação do conhecimento, também o faz para seu lado obscuro. A necessidade de informação imediata, devido à dependência digital, é conhecida como FOMO (*fear of missing out*, ou "medo de ficar de fora") e, infelizmente, tende a prevalecer sobre a análise fundamentada, porém diferida (Sampedro, 2021, p. 3). (DÍAZ CUESTA; GÓMEZ LÓPEZ; QUIÑONES DE LA IGLESIA, 2023, p. 227, tradução livre)

Nesse ínterim, é necessário pontuar que os algoritmos não são neutros. Eles ativamente selecionam, priorizam e amplificam certos tipos de conteúdo com base no modelo de negócios da atenção. Ocorre que essa curadoria automatizada tem efeitos diretos na forma como o público percebe e participa do debate social e político.

Bachur (2021, p. 445) ressalta que, na prática, os usuários das mídias digitais dificilmente conseguem discernir se as informações que consomem refletem de fato os problemas sociais mais relevantes, se as fontes são confiáveis ou se não se trata de desinformação. Essa dificuldade em filtrar informações com base em relevância, confiabilidade e proporção contribui para a fragmentação da esfera pública, criando as bolhas de filtro (*filter bubbles*) e as câmaras de eco (*echo chambers*), intensificando a polarização política resultante das interações nesse ambiente digital.

Além disso, a amplificação das emoções dos usuários é um dos efeitos diretos da lógica dos algoritmos, que recompensam conteúdos capazes de gerar fortes reações emocionais e interações intensas entre os usuários. Castro (2019, p. 20) retoma o conceito de Deleuze e Guattari, segundo o qual "as armas são afetos, e os afetos, armas", e destaca que emoções como

ódio, raiva, ressentimento e medo são favorecidas pelas plataformas algorítmicas, por gerarem maior engajamento e direcionarem-se a narrativas polarizantes e simplificadoras.

> O ódio é favorecido sobremaneira pelas plataformas algorítmicas, visto que está associado a maior engajamento. Ele ajusta-se à perfeição a narrativas simplificadoras, polarizantes, antissistema, direcionando-se diretamente àquilo que é demonizado por essas narrativas. Por outro lado, como demonstra a psicologia de massa de Freud (1967), o ódio dirigido a um alvo exterior funciona muito bem como motor de coesão de um grupo. Uma análise de cerca de 70 milhões de postagens de 278.654 usuários do Weibo, o equivalente chinês do Twitter, conclui que a raiva é significativamente mais influente que outras emoções, como a alegria (FAN et al., 2014). Avulta adicionalmente nas plataformas o ressentimento, que é próximo do ódio, como se fora uma mistura de ódio com inveja ou despeito. O ressentimento dirige-se preferencialmente àqueles que são encarados como receptores injustos de regalias, através, por exemplo, de programas sociais premiando indevidamente pessoas que estão no país ilegalmente, que não trabalham ou não se esforçam razoavelmente, que geram filhos sem ter condições de provê-los etc. Outro afeto marcante é o medo, explorado por meio de notícias que focalizam algo que possa representar uma ameaça para o sujeito. (CASTRO, 2019, p. 20)

Nesse aspecto, Bachur (2021, p. 455) aponta que a transição da mídia de *broadcasting* para as bolhas das redes sociais cria um ambiente em que os algoritmos amplificam a emoção coletiva, simulando uma "multidão *tailor-made*" para cada usuário. Desse modo, sentimentos como pertencimento, pressão de pares (*peer pressure*), viés de confirmação e a sensação de consenso são intensificados, propagando o contágio emocional característico das massas e provocando a regressão da consciência descrita por Freud (2011)[1].

Antes de avançar para a análise conceitual, é importante notar que os mesmos mecanismos descritos por Bachur — amplificação de emoções, simulação de uma multidão sob medida e regressão da consciência — criam um terreno fértil para a circulação de conteúdos enganosos.

Nesse ambiente, marcado pela lógica da economia da atenção e pela vulnerabilidade emocional dos usuários, a informação não é filtrada prioritariamente pela sua veracidade ou relevância pública, mas pela sua capacidade de mobilizar afetos. É nesse ponto que se insere a

[1] A regressão da consciência, segundo Freud, ocorre quando o indivíduo, sob influência de uma massa ou de emoções coletivas intensas, perde parcialmente sua capacidade de julgamento racional, passando a agir de forma mais impulsiva e dominada por afetos, facilitando o contágio emocional.

problemática da desinformação, cuja forma mais visível e popularizada se expressa na ideia de *fake news*.

De início, é necessário compreender que a desinformação deve ser entendida como um fenômeno social, estratégico e coletivo, e não apenas como a mentira individualizada. Segundo o Código de Conduta sobre Desinformação de 2022 da Comissão Europeia, trata-se de informação falsa ou enganosa, criada e disseminada com o objetivo de obter ganho econômico ou enganar intencionalmente o público, trazendo potencial de causar danos sociais, políticos ou individuais.

Entende-se que essa prática não é uma novidade da era digital: desde muito antes da internet, a desinformação foi utilizada como arma em conflitos e propagandas políticas. Todavia, o termo *fake news* ganhou popularidade em 2016, após as eleições presidenciais dos Estados Unidos. Ocorre que, embora útil em contextos midiáticos, a expressão é criticada por pesquisadores devido à sua ambiguidade e politização. Em muitos casos, prefere-se o uso do termo desinformação, por ser mais amplo e tecnicamente preciso.

> As notícias falsas sempre existiram na forma de propaganda ou de manchetes tendenciosas, semeando a confusão e o medo na opinião pública sobre temas sensíveis e concretos. Apesar disso, da ótica atual do indivíduo receptor, é fácil entender que se tenda a assimilar o termo fake news com propaganda, o que não é correto. Mas mais perigosa é a falta de conscientização sobre o fato de que o primeiro [termo] não comunica uma ideia precisa da magnitude do problema que as sociedades abertas enfrentam hoje em dia. (DÍAZ CUESTA; GÓMEZ LÓPEZ; QUIÑONES DE LA IGLESIA, 2023, p. 227, tradução livre)

Nesse viés, a confusão conceitual entre esses termos reduz a gravidade do problema, pois o rótulo *fake news* tende a banalizar uma ameaça que atinge diretamente a integridade das sociedades democráticas. Diante disso, aponta-se que a difusão de desinformação e *fake news* encontra no ambiente algorítmico das plataformas digitais um terreno fértil para sua propagação em larga escala.

Por meio da exposição dos usuários a conteúdos que reforçam suas crenças preexistentes, os algoritmos fornecem mecanismos que fortalecem seus vieses de confirmação, reduzindo a diversidade informacional e ampliando a impermeabilidade a visões divergentes.

Para além da personalização do ambiente digital onde verdadeiros usuários estão inseridos, os mecanismos de propagação da desinformação evoluíram para um ecossistema de alta sofisticação tecnológica, cujo principal campo de batalha é o ambiente virtual. Nesse

sentido, observa-se uma estratégia que geralmente se inicia com narrativas falsas criadas por agências específicas, que são então amplificadas em escala industrial por robôs automatizados (*bots*).

Ao simular um apoio popular inexistente, esses *bots* fabricam uma ilusão de consenso que pressiona a percepção individual. O verdadeiro objetivo dessa tática, no entanto, não é apenas a disseminação de um fato falso, mas a construção de um ambiente imersivo que sequestra a capacidade reflexiva do sujeito.

Segundo Moon e Gobbi (2024, p. 4), determinados movimentos constroem uma narrativa coletiva que insere o indivíduo em um pensamento de "enxame", reforçado pelo viés de confirmação, que leva à busca apenas por informações que validem crenças prévias. Esse processo é potencializado por estratégias de contrainteligência, como a produção de *fake news* e *memes*, caso semelhante ao "gabinete do ódio" no Brasil, de modo a forjar uma realidade na qual a verdade é fragmentada e manipulada como arma central da guerra informacional.

> Ela [a verdade] é volatilizada, segundo crenças individuais, a ser correspondida em pequenas parcelas nos acontecimentos diários, que reforcem no sujeito um viés de confirmação suficiente para que não haja espaço reflexivo para as informações circulando, apenas direções, instruções. Ao sujeito, o que vale é a construção de uma visão de mundo que se valide constantemente. Está aí o ponto mais crucial de uma guerra informacional: fazer o sujeito crer cada vez mais intensamente em uma realidade forjada. (MOON; GOBBI, 2024, p. 4)

Nesse processo, os cidadãos tornam-se, simultaneamente, sujeitos ativos e passivos: são manipulados por narrativas que exploram suas frustrações e medos e, ao mesmo tempo, contribuem ativamente para as campanhas de desinformação ao compartilharem o conteúdo falso em suas próprias redes.

Destaca-se ainda que, embora *bots* atuem como multiplicadores da desinformação, as pesquisas indicam que o maior vetor de viralização são os próprios usuários, justamente porque agem inflamados pelas emoções intensificadas pela desinformação e pelo compartilhamento em massa de notícias enganosas.

> No conflito atual na Ucrânia, o uso de algoritmos de inteligência artificial, a manipulação de sites que conectam os usuários ao subversor, a disseminação massiva de notícias falsas e narrativas por meio de programas de computador (bots) ou hackers humanos que atuam como usuários (trolls) formam um potente conjunto multiplicador de força em tempos de guerra, algo que está sendo visto de forma geral na atuação russa na Ucrânia. Isso pode gerar um

> arsenal militar também sobre o indivíduo ou grupos-alvo, de modo a sobrecarregar a capacidade de assimilação e torná-los incapazes de diferenciar a realidade dos conteúdos gerados ou de ficção. (DÍAZ CUESTA; GÓMEZ LÓPEZ; QUIÑONES DE LA IGLESIA, 2023, p. 229, tradução livre)

Nesse cenário, a exposição contínua a uma mesma narrativa, mesmo que falsa, gera o chamado efeito-verdade, no qual a familiaridade com uma afirmação aumenta a sua credibilidade. O ecossistema da desinformação online explora também a estratégia conhecida como *firehosing* ("mangueira de incêndio"), produzindo um estado de anomia informacional em que se torna cada vez mais difícil distinguir o verdadeiro do falso.

Sua operação se baseia em quatro pilares: primeiro, a emissão de um alto volume de conteúdo através de múltiplos canais diversificados; segundo, um processo de disseminação rápido, contínuo e repetitivo. Somam-se a isso as características do conteúdo em si: um total descompromisso com a realidade e, notavelmente, a ausência de consistência entre os discursos.

Ao inundar o ambiente informacional com uma torrente de informações contraditórias e sem lastro factual, essa tática torna cada vez mais difícil para o indivíduo distinguir o verdadeiro do falso, minando a confiança nas fontes e na própria noção de verdade. Assim, o impacto cumulativo desses mecanismos de propagação da desinformação não se limita à esfera informacional: ele se traduz em efeitos políticos e sociais.

3. FAKE NEWS E DEEPFAKES COMO ARMAS GEOPOLÍTICAS

A ascensão do ecossistema da desinformação online reconfigurou drasticamente o cenário dos conflitos internacionais. No século XXI, a disputa por hegemonia não se restringe mais aos campos de batalha tradicionais, estendendo-se ao ambiente virtual, onde a informação e a desinformação se tornaram armas estratégicas de imenso poder.

A exposição a conteúdos enganosos provenientes do ambiente digital altamente influenciado pela personalização dos algoritmos não apenas consolida opiniões, mas frequentemente radicaliza posições. Em grupos fechados, a lógica algorítmica e a dinâmica emocional alimentam uma espiral de extremismo, reduzindo o espaço para consensos e diálogos democráticos. Esse processo, contudo, não se manifesta de forma simétrica nos diferentes espectros políticos.

Segundo a análise de Castro (2019, p. 17-18), embora as plataformas algorítmicas se apresentem como uma ágora supostamente neutra, seu equilíbrio é ilusório e inevitavelmente dá margem a desequilíbrios que induzem à polarização. O autor defende que essa polarização

ganha um caráter assimétrico com a ascensão de máquinas de guerra híbrida. Para Castro, a assimetria se estabelece, primeiramente, porque um dos polos "se alimenta de uma dieta informacional mais homogênea, o que lhe dá maior consistência ideológica" (2019, p. 18).

Essa coesão permite que um lado se organize como uma insurgência, com um nível de coordenação, força e belicosidade que falta a seus adversários, criando uma clara desproporção de poder discursivo. Assim, o espaço que aspirava ser um "condomínio" ou "*shopping center*" de ideias vira campo de batalha. Esse fenômeno, conclui Castro (2019, p. 18) ao citar Virilio, solapa a política tradicional e instaura uma "transpolítica", que não é mais assentada no diálogo.

Nesse contexto, a lógica da política se aproxima da lógica da guerra: a desinformação se converte em munição simbólica, utilizada para corroer instituições, enfraquecer a confiança pública e transformar o espaço democrático em campo de batalha permanente. Nesse ínterim, as *fake news* foram incorporadas como armas geopolíticas, servindo como ferramenta central para a desestabilização de governos e a promoção de interesses geopolíticos.

Segundo o entendimento de Korybko (2018), a guerra híbrida é definida como um novo modelo de guerra indireta, uma estratégia de desestabilização e troca de regime utilizada pelos Estados Unidos no século XXI para substituir governos não alinhados à sua política. Assim, o conceito de guerra híbrida consolidou-se porque captura a fusão de táticas antigas de propaganda e subversão com as novas tecnologias digitais, explicando como atores estatais e não estatais podem travar conflitos de forma indireta, contínua e desestabilizadora, desafiando as noções tradicionais de guerra e segurança.

Em sentido lato, consiste em um conjunto de ações que minimizam ou eliminam a necessidade de operações bélicas diretas, tornando o processo de subversão menos custoso e politicamente mais defensável. Desse modo, o conceito de guerra híbrida oferece um vocabulário e um quadro analítico para entender uma realidade geopolítica transformada. A partir dele, é possível compreender melhor a desinformação como arma geopolítica.

Para este estudo, a análise da guerra híbrida parte do conceito de revolução colorida, a qual, segundo Korybko (2018), é o primeiro elemento da "combinação entre revoluções coloridas e guerras não convencionais". Conhecida como "golpe brando", esta é uma fase essencialmente político-informacional, cujo propósito é a mudança de regime por meio de estratégias aparentemente não violentas, como o uso da desinformação para catalisar protestos em massa.

> O principal objetivo da campanha de informação é que o alvo internalize as ideias que lhe são apresentadas, dando a impressão de que os próprios

> manifestantes chegaram, por conta própria, às conclusões induzidas de fora. As ideias contra o governo devem parecer espontâneas e não forçadas, dando-se grande ênfase à abordagem indireta para comunicá-las. Se as pessoas perceberem que estão sendo manipuladas por mãos invisíveis, elas rejeitarão em massa a mensagem. Se, contudo, for possível internalizar essa mensagem em uma pessoa e ela começar a difundi-la para seus amigos íntimos e pessoas próximas, que jamais sequer imaginariam que essa pessoa está sob influência involuntária de uma operação psicológica estrangeira, então o vírus de Mann contaminará a sociedade e começará a espalhar as ideias da revolução colorida por conta própria. (KORYBKO, 2018, p. 50)

Tal estratégia consubstancia-se no que se pode denominar "caos administrado" (KORYBKO, 2018, p. 35), tendo o ecossistema de desinformação online como uma de suas ferramentas. Sob os imperativos da economia da atenção, em que a capacidade de viralização constitui a métrica de eficácia, as plataformas de redes sociais são instrumentalizadas com o fito de erodir a legitimidade do *status quo*, inclusive com a exploração dos dados coletados por meio da personalização algorítmica.

Nesse sentido, o objetivo tático transcende a mera imposição coercitiva de uma ideia; busca-se, antes, criar as condições para que o público-alvo internalize a mensagem, de modo que conclusões exogenamente induzidas sejam percebidas como cognições autônomas e espontâneas.

Para a consecução de tal internalização, a mobilização popular é articulada em torno de pautas generalistas e de elevado capital afetivo — a exemplo da "defesa da democracia" ou do "combate à corrupção". Assim, conteúdos desinformativos e narrativas simplificadas são deliberadamente arquitetados para se disseminarem por capilaridade através de redes sociais, cujo compartilhamento interpessoal dissimula a sua gênese e o seu propósito estratégico.

Deste modo, embora tais mobilizações ostentem a aparência de manifestações orgânicas da "sociedade civil", elas frequentemente decorrem de uma articulação estratégica financiada e assessorada por atores exógenos, os quais se valem da arquitetura do ecossistema digital para orquestrar a dissidência.

> Embora seja usada nas duas etapas, é na revolução colorida que tal ferramenta [fake news] surte mais efeito. Afinal, antes mesmo de se instaurar de fato o referido processo, a nação imperialista já objetiva conquistar "corações e mentes", realizando uma mudança no pensamento da população do país alvo, através de guerras de informação e psy-ops (operações psicológicas) (Freitas, 2019, p. 11). Nesse sentido, cria-se uma rede massiva de propagação de fake news, até que se chegue a um momento no qual grande parte dos cidadãos não

> saiba mais o que é verdade ou mentira (Souza, 2020, p. 157). (OLIVEIRA DA SILVA; CARBONE ANVERSA; DELGADO DE DAVID, 2021, p. 10)

Na eventualidade de a revolução colorida não lograr êxito na deposição do governo-alvo, a estratégia insurrecional transita para sua segunda fase, a Guerra Não Convencional ou "golpe rígido". Esta etapa é marcada por uma escalada para a beligerância aberta, caracterizada pela instrumentalização de forças não regulares — tais como guerrilhas e grupos insurgentes — cujo escopo é a implosão do aparato estatal.

Ademais, é imperativo compreender que esta fase não constitui uma ruptura, mas uma progressão orgânica da precedente, valendo-se do capital social e das redes de mobilização previamente consolidadas como substrato para a insurgência armada. Cumpre salientar, contudo, que embora a compreensão dessa escalada militar seja pertinente, o escopo analítico deste trabalho circunscreve-se à fase inaugural da guerra híbrida, a revolução colorida, de natureza eminentemente político-informacional.

A guerra híbrida que culminou na deposição de Evo Morales na Bolívia em 2019 teve como um de seus antecedentes o plebiscito de 2016 sobre a reeleição presidencial. Na ocasião, a derrota do então presidente foi decisivamente influenciada pela disseminação massiva de desinformação, como a falsa notícia sobre um suposto filho secreto, no que ficou conhecido como "Caso Zapata".

O episódio demonstrou o uso da manipulação psicológica para influenciar resultados democráticos, conforme expõem Oliveira da Silva, Carbone Anversa e Delgado de David (2021, p. 11):

> Em 2016, por exemplo, às vésperas do plebiscito que consultou a população sobre a possibilidade de Evo Morales concorrer a mais um mandato, a oposição propagou inúmeras notícias falsas, sendo que a mais debatida era que o presidente tinha um filho com Gabriela Zapata e que tentara esconder a morte da criança. Outras acusações afirmavam que o filho de Morales estava em "exílio" no exterior, visando a sua segurança. Todavia, após uma série de investigações, descobriu-se que, na realidade, a referida criança nunca sequer existiu (Valença, 2017, apud El Cartel de la Mentira, 2016). Essa notícia e o cenário de incerteza e caos gerado por ela foram, em grande medida, responsáveis pela perda de Morales no plebiscito, o qual influenciou significativamente no desenrolar do golpe. Desse modo, entende-se que a influência do "caso Zapata" se deu, principalmente, por questões psicossociais. Afinal, a relação do indivíduo com os fatores que o circundam é determinante para a formação da identidade subjetiva, uma vez que é a partir disso que se cria uma noção de responsabilidade (Barbosa, 2018). Nesse sentido, a oposição política de Morales, estrategicamente, aproveitou-se desse

> sentimento de obrigação para com o outro e de indignação (os quais são ainda mais intensos por se tratar de uma notícia envolvendo criança) para "conquistar corações e mentes", característica central da Guerra Híbrida. (OLIVEIRA DA SILVA; CARBONE ANVERSA; DELGADO DE DAVID, 2021, p. 11)

Portanto, a análise do caso boliviano transcende o estudo de um golpe de Estado isolado, servindo como um alerta sobre a vulnerabilidade das democracias contemporâneas. A instrumentalização das redes sociais tornou-se o vetor central dessas novas táticas, onde a disseminação de desinformação é exponencialmente acelerada por algoritmos projetados para maximizar o engajamento e por sistemas de inteligência artificial que automatizam a manipulação em larga escala.

4. A INTELIGÊNCIA ARTIFICIAL E A CRISE DA AUTENTICIDADE

Sabe-se que a economia da atenção moldou as plataformas digitais, que utilizam algoritmos para maximizar o engajamento, resultando em uma amplificação que favorece a polarização e a desinformação. Contudo, essa dinâmica atinge outro patamar quando o motor dessa amplificação deixa de ser apenas um algoritmo de recomendação e passa a ser a inteligência artificial.

A IA não se limita a disseminar narrativas falsas, ela agora possui a capacidade de gerá-las em escala industrial, por meio de *bots* e da manipulação de conteúdo. É justamente essa transição — da simples disseminação de mentiras para a fabricação sintética de realidades — que lança a sociedade em uma profunda crise da autenticidade, cujas dimensões e consequências serão exploradas neste capítulo.

Ao mesmo tempo em que oferece avanços em inúmeros campos, a IA emerge como a principal ferramenta em um conflito cada vez mais difuso e perigoso: a guerra da informação. Especialmente por meio da geração de conteúdo sintético como os *deepfakes*, a IA precipitou uma crise de autenticidade, desafiando a capacidade do indivíduo de distinguir o real do fabricado e ameaçando os alicerces da confiança social e da estabilidade democrática.

Nesse viés, a era da informação, paradoxalmente, consolidou-se também como a era da desinformação (DÍAZ CUESTA; GÓMEZ LÓPEZ; QUIÑONES DE LA IGLESIA, 2023, p. 226, tradução livre). A digitalização e a ascensão das redes sociais já haviam acelerado exponencialmente a velocidade e o alcance de narrativas falsas, mas a Inteligência Artificial

representa uma mudança de paradigma, uma transformação qualitativa, e não apenas quantitativa, nesse cenário.

Anteriormente, a disseminação massiva de desinformação dependia de ferramentas como algoritmos de recomendação, manipulação de sites, exércitos de *bots* e *trolls* (agentes humanos). Embora eficazes, essas operações exigiam recursos significativos e, muitas vezes, deixavam rastros detectáveis. A chegada da IA generativa subverteu essa lógica. Agora, é possível criar conteúdo falso — textos, áudios, imagens e vídeos — em escala industrial, a um custo irrisório e com um grau de verossimilhança que desafia a percepção humana.

O imediatismo inerente às redes sociais cria uma demanda por conteúdo que seja interativo e visualmente impactante. Nesse cenário, a inteligência artificial funciona como um acelerador para a produção desses materiais, embora nem sempre com fins informativos. De acordo com Torres Morales e Viteri Torres (2025, p. 7613), existe uma produção de conteúdo especificamente voltada para a distorção de fatos, cujo propósito final é a desinformação.

A desinformação gerada por Inteligência Artificial, incluindo tecnologias de *deepfake*, foi categorizada pelo Fórum Econômico Mundial (2025) como um risco proeminente à estabilidade global nos próximos anos. O impacto dessa tecnologia transcende a mera influência em eleições ou ataques a reputações individuais, seu objetivo estratégico é corroer a própria percepção da realidade compartilhada. Ao minar a confiança nas instituições, na mídia e nos processos democráticos, essa nova forma de desinformação amplifica a discórdia social e a polarização.

A desinformação, posicionada pelo segundo ano consecutivo como a principal preocupação global a curto e médio prazo, conforme o relatório do Fórum Econômico Mundial (2025, p. 4) revela um percalço nos esforços para seu combate: o conteúdo falso ou enganoso criado por Inteligência Artificial Generativa, que pode ser produzido e distribuído em larga escala.

Tem-se então o epicentro da atual crise de autenticidade: os *deepfakes*, conteúdos de mídia gerados por IA que pretendem se assemelhar a pessoas, objetos ou eventos reais. Eles são a manifestação mais visível e perturbadora desse novo poder tecnológico. Os *deepfakes* não apenas distorcem a realidade, como o faziam as fotomontagens ou os vídeos editados do passado, eles criam realidades próprias, desconectando completamente o público dos fatos. Em um ecossistema informacional saturado por *deepfakes*, a verdade objetiva perde relevância, o que importa é aquilo que a audiência é levada a acreditar como real.

A crescente sofisticação da IA generativa cria um verdadeiro arsenal informacional que se abate sobre o cidadão comum, tornando-o incapaz de diferenciar a realidade de

conteúdos ficcionais. O impacto na democracia e na esfera pública é direto e corrosivo: sem uma base factual compartilhada, o debate racional se torna inviável e a confiança, pilar de qualquer sociedade funcional, é erodida.

Este fenômeno é o que Pawelec (2022, p. 12) conceitua como "decadência da confiança informacional". Segundo a autora, quando o discurso democrático não pode mais se apoiar em fatos e verdades compartilhados, a deliberação perde sua função epistêmica, ou seja, sua capacidade de gerar decisões de qualidade. Consequentemente, a formação coletiva da agenda e da vontade, um processo central para a democracia, é distorcida e obstruída, desestabilizando o ambiente cognitivo essencial para a tomada de decisões políticas informadas.

Tem-se então um estado de confusão e desorientação que é, precisamente, o objetivo da propagação deliberada da desinformação como arma geopolítica. O propósito final, conforme teorizado em doutrinas de guerra híbrida, é induzir uma paralisia cognitiva na sociedade-alvo.

Um público desorientado e fragmentado torna-se incapaz de formular respostas coesas e racionais a crises, facilitando a manipulação externa e a desestabilização de processos democráticos. Desta forma, a desinformação transcende a propaganda tradicional e se consolida como uma arma estratégica que ataca um dos pilares da democracia: a necessidade de uma base factual compartilhada para o debate público e a tomada de decisão informada.

5. O VAZIO NORMATIVO BRASILEIRO E A VANGUARDA EUROPEIA NA REGULAÇÃO DE DEEPFAKES

O reconhecimento de que a desinformação funciona como uma arma estratégica, projetada para atacar os pilares da democracia, impulsionou a busca por soluções regulatórias em escala global. Nessa conjuntura, a União Europeia (UE) está a lidar com a desinformação por *deepfakes* e a regulação da Inteligência Artificial (IA) por meio de uma abordagem jurídica pioneira, centrada principalmente em dois pilares legislativos: o *AI Act* (Lei de Inteligência Artificial) e o *Digital Services Act* (DSA - Lei de Serviços Digitais).

Segundo Förster *et al*. (2025, p. 3), o *AI Act* visa regulamentar os sistemas de IA na União Europeia, bem como seus fornecedores e implementadores, por meio de uma abordagem baseada em risco. A partir de agosto de 2026, a legislação obrigará a divulgação de que um conteúdo foi gerado ou manipulado por sistemas de IA. O artigo 50 do *AI Act* divide a obrigação de transparência para *deepfakes* entre os fornecedores do sistema de IA, que devem aplicar uma

marcação em formato legível por máquina, e os implementadores (quem utiliza o sistema), que devem garantir que o conteúdo seja claramente reconhecido como um *deepfake*.

Ainda de acordo com os autores, um dos objetivos dessa exigência é facilitar o cumprimento das obrigações do *Digital Services Act*. O DSA foca na regulação de serviços intermediários, como redes sociais e motores de busca. No contexto dos *deepfakes*, suas obrigações de transparência mais relevantes aplicam-se apenas ao nível mais alto, ou seja, às plataformas online muito grandes (*Very Large Online Platforms* - VLOPs) e aos motores de busca muito grandes (*Very Large Online Search Engines* - VLOSEs), que serão obrigados a rotular explicitamente tais conteúdos.

Assim, buscando mitigar os riscos associados aos *deepfakes*, a União Europeia aprovou regulações que exigem transparência por parte dos fornecedores e implementadores de sistemas de IA, bem como das plataformas online (Förster et al., 2025, p. 1). Contudo, a implementação dessas medidas enfrenta um desafio gigantesco: a detecção.

Conforme explica Förster et al. (2025, p. 6), a obrigação de rotulagem (*labeling*) imposta pelo DSA é consideravelmente mais complexa de ser cumprida do que a de marcação (*marking*) exigida pelo *AI Act*. A razão para isso é que as plataformas não conseguem rastrear com segurança a origem do conteúdo gerado por terceiros. Elas não têm como garantir que materiais produzidos por usuários fora da União Europeia — que não estão sujeitos às regras do *AI Act* — ou mesmo por aqueles que não cumprem a lei dentro da UE, chegarão com a devida marcação de origem.

Como consequência, antes mesmo de poderem rotular os *deepfakes*, as plataformas são obrigadas a desenvolver suas próprias e robustas estruturas de detecção, o que, na prática, dá início a uma complexa "corrida armamentista" tecnológica. Os geradores de *deepfakes* evoluem constantemente para evadir a detecção, e os detectores precisam ser continuamente atualizados para acompanhá-los. Portanto, um sistema de detecção eficaz torna-se um pré-requisito para o sucesso da regulação proposta pela União Europeia.

Enquanto a abordagem europeia avança com regulações específicas e tecnológicas, focando em riscos e atores distintos, o Brasil seguiu um caminho contrastante, que ilustra os perigos de uma estratégia regulatória excessivamente ampla e unificada, deixando o país em um estado de vácuo normativo.

A recente experiência brasileira ilustra uma abordagem fundamentalmente distinta e, ao final, malsucedida. O Brasil tentou resolver o crescente problema das *fake news* focando na regulação ampla das plataformas digitais através do Projeto de Lei 2.630/2020. A trajetória do projeto, que se expandiu de um objetivo inicial restrito para uma ambiciosa tentativa de

enquadrar todo o heterogêneo ecossistema digital sob uma única lei, provocou uma reação intensa e previsível.

Ao se sentirem ameaçadas por um modelo que não distinguia suas operações, grandes empresas de tecnologia, como o Google, utilizaram seu poder de mercado e suas próprias plataformas para se opor à proposta. O então Diretor de Relações Governamentais do Google Brasil, Marcelo Lacerda (2023), evidenciou essa preocupação ao afirmar que, na versão discutida do projeto, "os mecanismos de pesquisa são tratados da mesma forma que as redes sociais e os serviços de mensagens instantâneas", o que, segundo ele, "acaba causando uma distorção que prejudica a Busca".

Essa percepção de um tratamento inadequado e perigoso para seu modelo de negócio motivou uma campanha pública de oposição. A empresa não apenas publicou sua posição em seu blog oficial, mas também convocou ativamente seus usuários a pressionarem o legislativo, demonstrando o uso de sua plataforma para influenciar o debate. A combinação de uma estratégia legislativa excessivamente abrangente com o *lobby* empresarial levou a um impasse de quatro anos, culminando no arquivamento do projeto.

O resultado dessa tentativa fracassada não foi apenas a não resolução do problema original da desinformação, mas também a consolidação de um perigoso vácuo regulatório. Agora, o Brasil se encontra legalmente despreparado para a nova e mais complexa fase deste desafio: a ascensão da Inteligência Artificial generativa, que não só amplificou a escala da desinformação, mas também introduziu uma categoria de ameaça inteiramente nova e mais potente, os *deepfakes*, para a qual o arcabouço jurídico nacional carece de ferramentas específicas.

O vácuo regulatório deixado pelo arquivamento do PL 2.630/2020, contudo, não significa uma paralisia legislativa completa. Pelo contrário, o fracasso em aprovar uma única e abrangente lei parece ter redirecionado os esforços do Congresso para uma abordagem mais segmentada e específica, focando diretamente nas tecnologias emergentes e em seus usos mais danosos, em vez de tentar regular todo o ecossistema digital de uma só vez.

Nesse novo cenário, a iniciativa mais importante é o Projeto de Lei 2.338/2023, que propõe o Marco Legal da Inteligência Artificial. Já aprovado no Senado e em tramitação na Câmara dos Deputados, o projeto é inspirado no *AI Act* da União Europeia e adota uma abordagem baseada em níveis de risco. Seu objetivo é estabelecer um arcabouço de direitos, transparência e responsabilidade para o desenvolvimento e uso da IA no país, prevendo inclusive a proteção e remuneração de direitos autorais.

Paralelamente, o legislador tem atuado de forma reativa para combater a ameaça imediata dos *deepfakes*. Em abril de 2025, foi sancionada a Lei 15.123/2025 para estabelecer uma causa de aumento de pena no crime de violência psicológica contra a mulher quando este for cometido por meio do uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima.

Com a nova redação, ficou determinado que, nesses casos, a pena para o crime é aumentada de metade, reconhecendo o potencial agravado do dano causado por ferramentas como *deepfakes*, que frequentemente resultam em humilhação pública, isolamento social e sérios traumas psicológicos nas vítimas. Esta medida se soma a normas já existentes no âmbito eleitoral, em que resoluções do Tribunal Superior Eleitoral (TSE) preveem a cassação de mandatos em casos de uso de *deepfakes* para disseminar desinformação.

Portanto, embora o Brasil ainda não possua uma lei nacional abrangente e sancionada sobre Inteligência Artificial, o caminho regulatório está em plena evolução. Diferentemente da tentativa malfadada do PL 2.630/2020, a estratégia atual, dividida entre um marco geral para a IA e leis específicas para seus usos ilícitos, demonstra um amadurecimento do debate. O Brasil avança, ainda que tardiamente, para construir as ferramentas jurídicas necessárias para enfrentar a complexidade da guerra informacional na era da IA.

6. CONSIDERAÇÕES FINAIS

O presente estudo se propôs a identificar de que maneira a ausência de regulação da inteligência artificial e das plataformas digitais no Brasil impacta a segurança e a estabilidade democrática diante da disseminação de desinformação. A resposta, obtida por meio da análise aqui desenvolvida, é que a ausência de um arcabouço regulatório específico impacta a segurança de forma direta, ao deixar o país estrategicamente vulnerável.

O vácuo normativo permite que a desinformação, potencializada por tecnologias como *deepfakes*, seja empregada como arma em estratégias de guerra híbrida sem que haja ferramentas jurídicas adequadas para detecção, responsabilização e mitigação de danos em escala. Na prática, o Brasil se torna um alvo mais suscetível a operações de desestabilização interna e manipulação da opinião pública, o que corrói a confiança e fragiliza os pilares do regime democrático.

Os resultados da investigação confirmam, portanto, a hipótese inicial de que a carência de leis específicas amplia a vulnerabilidade do país em comparação a blocos com marcos jurídicos mais consolidados, como a União Europeia. O estudo demonstrou que o vácuo

normativo brasileiro não é um mero atraso, mas a consequência de uma estratégia regulatória equivocada, materializada no fracassado Projeto de Lei 2.630/2020. A tentativa de criar uma lei monolítica revelou-se um caminho inviável, que, ao final, deixou o país despreparado para a escalada tecnológica da desinformação.

Diante do exposto, este trabalho conclui que a resposta mais eficaz para mitigar os riscos identificados reside em uma fundamental mudança de paradigma: é preciso abandonar a ideia de "regular plataformas" e adotar a estratégia de regular atividades realizadas no ambiente digital. Assim como o Direito tradicional se especializa em áreas como civil e penal, a regulação do ambiente digital deve ser segmentada para tratar de problemas específicos com a precisão necessária. Nesse modelo, a manipulação algorítmica de conteúdo, por exemplo, seria objeto de uma regulação própria, impondo deveres de transparência e mitigação de riscos a qualquer serviço que utilize tais sistemas.

Sugere-se, assim, que uma abordagem baseada em atividades, em vez de plataformas, representa uma alternativa viável, contribuindo para a criação de um arcabouço jurídico mais flexível e resiliente. Ao focar na ação e no dano potencial, e não no agente, o Brasil teria melhores condições de construir uma legislação capaz de se adaptar às inovações tecnológicas. Argumenta-se, por fim, que esta pode ser uma via para o desenvolvimento de uma defesa mais robusta e inteligente, apta a reduzir a vulnerabilidade do país e a salvaguardar a democracia na era da guerra informacional.

7. REFERÊNCIAS BIBLIOGRÁFICAS

BACHUR, João Paulo. Desinformação política, mídias digitais e democracia: Como e por que as fake news funcionam?. **Direito Público**, *[S. l.]*, v. 18, n. 99, 2021. DOI: 10.11117/rdp.v18i99.5939. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/5939. Acesso em: 30 set. 2025.

CASTRO, Julio Cesar Lemes de. Máquinas de guerra híbrida em plataformas algorítmicas. **E-Compós**, *[S. l.]*, v. 23, 2020. DOI: 10.30962/ec.1929. Disponível em: https://www.e-compos.org.br/e-compos/article/view/1929. Acesso em: 30 set. 2025.

COMISSÃO EUROPEIA. **The 2022 Code of Practice on Disinformation**. 31 jul. 2025. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation. Acesso em: 30 set. 2025.

DÍAZ CUESTA, José Francisco; GÓMEZ LÓPEZ, Jacinto; QUIÑONES DE LA IGLESIA, Javier. La desinformación y la guerra híbrida: Instrumentalización de las narrativas informativas para entender la guerra del siglo XXI. **Comunicación y Hombre**, *[S. l.]*, n. 19, p. 223-232, 2023. Disponível em:

https://portalderevistas.ufv.es/index.php/comunicacionyhombre/article/view/757. Acesso em: 30 set. 2025.

FÖRSTER, Max-Paul; DECK, Luca; WEIDLICH, Raimund; KÜHL, Niklas. **A Multi-Level Strategy for Deepfake Content Moderation under EU Regulation**. Disponível em: https://arxiv.org/abs/2507.08879. Acesso em: 30 set. 2025.

FÓRUM ECONÔMICO MUNDIAL. **Global Risks Report 2025**. Cologny: Fórum Econômico Mundial, 2025. Disponível em: https://www.weforum.org/publications/global-risks-report-2025/. Acesso em: 30 set. 2025.

FREUD, Sigmund. **Psicologia das massas e análise do eu e outros textos (1920-1923)**. Tradução de Paulo César de Souza. São Paulo: Companhia das Letras, 2011.

KORYBKO, Andrew. Guerras híbridas: das revoluções coloridas aos golpes. Tradução de Thyago Antunes, 1. ed. São Paulo: Expressão Popular, 2018.

LACERDA, Marcelo. Como o PL 2630 pode piorar a sua internet. **Blog do Google Brasil**, 27 abr. 2023. Disponível em: https://blog.google/intl/pt-br/novidades/iniciativas/como-o-pl-2630-pode-piorar-a-sua-internet/. Acesso em: 30 set. 2025.

MOON, Rodrigo Malcom de Barros; GOBBI, Maria Cristina. A comunicação e a informação sob influência da guerra híbrida. **Intercom, Revista Brasileira de Ciências da Comunicação.**, São Paulo, v. 47, 2024. Disponível em: https://www.scielo.br/j/interc/a/t9dhfkgFBqT5TtNbHtFQjwg/?format=html&lang=pt. Acesso em: 30 set. 2025.

OLIVEIRA DA SILVA, Maria Beatriz; CARBONE ANVERSA, Ana Elisi; DELGADO DE DAVID, Thomaz. A Instrumentalização das Fake news nas Guerras Híbridas: uma análise a partir do Golpe na Bolívia (2019). **Mural Internacional**, Rio de Janeiro, v. 12, 2021. Disponível em: https://www.e-publicacoes.uerj.br/muralinternacional/article/view/60375. Acesso em: 30 set. 2025.

PAWELEC, Maria. Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions. **Digital Society**, *[S. l.]*, v. 1, n. 19, p. 1-37, set. 2022. Disponível em: https://link.springer.com/article/10.1007/s44206-022-00010-6. Acesso em: 30 set. 2025.

TORRES MORALES, Alex Fabricio; VITERI TORRES, Walter. Impacto de la IA Inteligencia Artificial en el Consumo de la Información sobre Geopolítica. **Ciencia Latina Revista Científica Multidisciplinar**, v. 9, n. 3, p. 7611-7632, 16 jul. 2025. Disponível em: https://ciencialatina.org/index.php/cienciala/article/view/18387. Acesso em: 30 set. 2025