

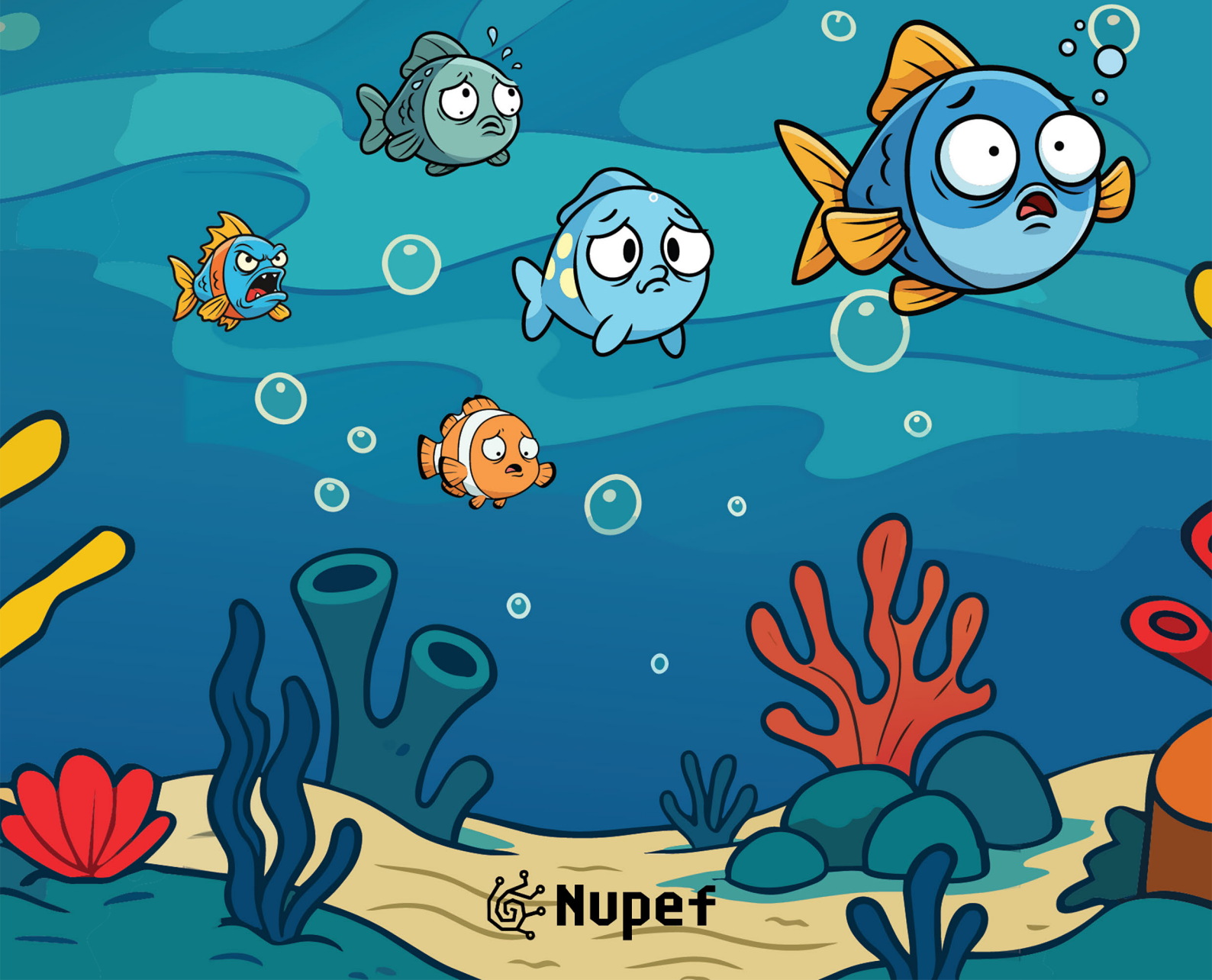
# POLITICS

Uma publicação do Nupef [ nupef.org.br ] jul. 2025

## O Avanço do DeepSeek

O professor Charles Mok faz um relato minucioso sobre o surgimento do DeepSeek, que causou um terremoto no espaço de desenvolvimento dos chamados "Large Language Models"

Novas contribuições à consulta pública do CGI.br sobre regulação de plataformas digitais no Brasil





# POLITICS

[ <https://politics.org.br> ]

# POLITICS

Uma publicação do Nupef [ [nupef.org.br](http://nupef.org.br) ] jul. 2025

## COMISSÃO EDITORIAL DESTA EDIÇÃO

RAFAEL EVANGELISTA  
LISANDRO GRANVILLE  
BIANCA KREMER  
MARCELO FORNAZIN  
RODOLFO AVELINO

## EDITOR

CARLOS A. AFONSO

## ORGANIZAÇÃO DA EDIÇÃO

RAFAEL EVANGELISTA (UNICAMP/CGI.BR)  
JULIANO CAPPI (CGI.BR)  
JULIANA OMS (CGI.BR)  
OONA CASTRO (NUPEF)

## ASSESSORIA EDITORIAL/APOIO TÉCNICO

ÉRICA S. DE FREITAS (PREPARAÇÃO E REVISÃO TEXTUAL)  
CARLOS A. AFONSO (PREPARAÇÃO E REVISÃO TEXTUAL)  
LAILA A. BRAGA (GESTÃO DO SISTEMA DE SUBMISSÕES)  
JOYCE SOUZA (GESTÃO DO PROCESSO DE AVALIAÇÕES)

## CAPA E PROJETO GRÁFICO

PAULO DUARTE

## COMITÊ CONSULTIVO DA POLITICS(\*) AVRI DORIA • CARLOS

AFFONSO PEREIRA DE SOUZA • DEIRDRE WILLIAMS • DEMI  
GETSCHKO • GRACIELA SELAIMEN • JEREMY MALCOLM •  
JOÃO BRANT • LOUIS POUZIN • MARILIA MACIEL • MAWAKI  
CHANGO • VALERIA BETANCOURT

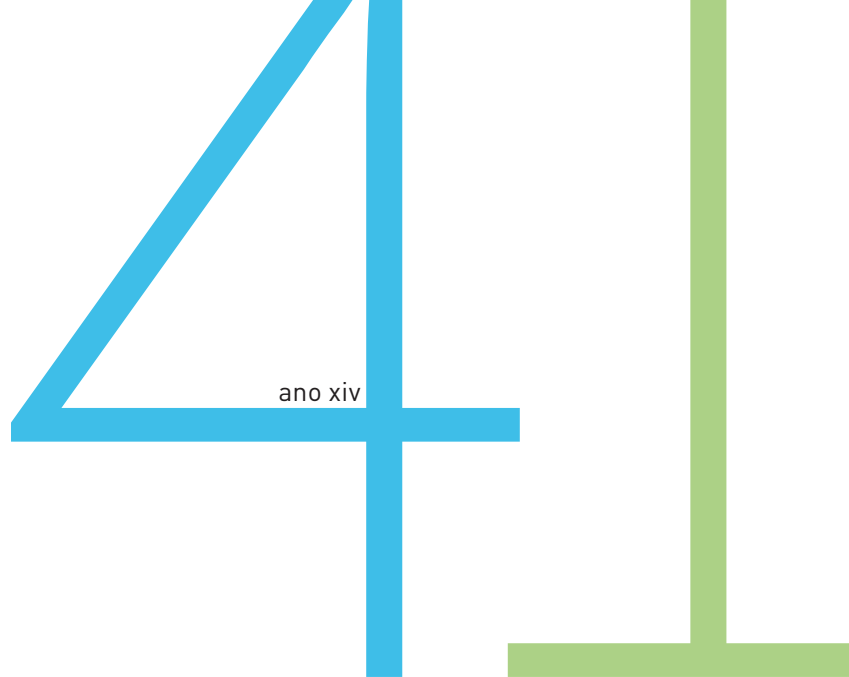
*(\*) Mais detalhes sobre os membros do Comitê Consultivo  
em <https://politics.org.br>*

Os textos publicados aqui são de responsabilidade de seus  
autores, não necessariamente representando os pontos de  
vista das entidades às quais estão vinculados, salvo indica-  
ção explícita em contrário.

A tiragem das nossas edições é pequena. Se você quiser  
receber gratuitamente a edição impressa, envie um e-mail  
para [politics@nupef.org.br](mailto:politics@nupef.org.br) com seu nome, endereço  
completo - incluindo o CEP - e a sua área de atuação.

Todas as edições da POLITICS estão disponíveis em [politics.org.br](http://politics.org.br)

A POLITICS procura aderir à terminologia e abreviaturas do Sistema Internacional de Unidades (SI), adotado pelo Instituto Nacional de Metrologia do Brasil (Inmetro). Assim, todos os textos são revisados para assegurar, na medida do possível e sem prejuízo ao conteúdo, aderência ao SI. Para mais informação: <http://www.inmetro.gov.br/consumidor/unidLegaisMed.asp>

**ATRIBUIÇÃO**

Você deve dar crédito ao autor original, da forma especificada pelo autor ou licenciante.

**USO NÃO-COMERCIAL**

Você não pode utilizar esta obra com finalidades comerciais.

**VEDADA A CRIAÇÃO DE OBRAS DERIVADAS**

Você não pode alterar, transformar ou criar outra obra com base nesta.

*Para cada novo uso ou distribuição, você deve deixar claro para outros os termos da licença desta obra.*

*Qualquer uma destas condições podem ser renunciadas, desde que você obtenha permissão do autor.*

**E**sta edição da poliTICs traz quatro textos que debatem os resultados da consulta do CGI.br sobre regulação de plataformas digitais no Brasil, realizada em 2023. A consulta originalmente recebeu um total de 1.336 contribuições de pessoas e organizações dos quatro setores que compõem o CGI.br (setor governamental, terceiro setor, setor empresarial e comunidade científica e tecnológica). Em seguida, o CGI.br publicou um relatório de sistematização dos resultados, para apresentá-los de forma mais acessível e sintética. No entanto, as extensas contribuições dadas pela sociedade brasileira permitem diversas interpretações e análises por metodologias diversas, que podem ser exploradas por novos autores.

Uma nova chamada de contribuições foi então realizada pelo CGI.br, em parceria com o Nupef, com o objetivo de publicar os textos melhor avaliados, em um processo de revisão por pares, na revista poliTICs. Das mais de 60 contribuições, 14 artigos foram aprovados e selecionados para publicação da edição 40. Devido ao tamanho para publicação impressa, a edição especial da poliTICs foi publicada em dois volumes com o apoio do CGI.br. Os artigos restantes seguirão sendo analisados pela equipe editorial da poliTICs para futura publicação conforme o interesse das/os autoras/es.

O Nupef decidiu selecionar mais quatro artigos para a edição 41, e planeja criar um espaço no site da revista para acomodar todas as outras contribuições, desde que autorizadas pelos/as autores/as. Abaixo um resumo dos artigos:

**Transparência de Dados em Conteúdos de Interesse Público: Propostas de Regulação para Plataformas Digitais no Brasil** (Rodrigo Moreira dos Santos)

O estudo investiga as lacunas na capacitação profissional e apresenta propostas práticas para fortalecer a regulação digital no Brasil. A pesquisa destaca a neces-

sidade de currículos interdisciplinares que integrem tecnologia, direito e ética, bem como programas de certificação e parcerias público-privadas para expandir o acesso ao conhecimento especializado.

### **Transparência de Dados em Conteúdos de Interesse Público: Propostas de Regulação para Plataformas Digitais no Brasil** (Eliandro Jeovane Natal da Silva)

O artigo explora a necessidade de maior transparência de dados em conteúdos de interesse público nas plataformas digitais, regulamentações mais claras e rigorosas sobre o uso de dados pessoais, e a moderação de conteúdo. Com base na análise das contribuições da consulta pública do CGI.br (2023), propõe-se a implementação de uma governança mais robusta e transparente, que deve incluir regulações precisas e rigorosas sobre o uso de dados pessoais e a moderação de conteúdo, assegurando o equilíbrio entre interesses comerciais e a proteção dos direitos fundamentais dos usuários.

### **Mídias sociais, regulação processual e dever de cuidado: evidências empíricas do debate no Brasil** (Ivar Hartmann, Ramon Costa, Bruno Oliveira)

Investiga a regulação de plataformas digitais no Brasil, com foco na discussão do dever de cuidado nesse contexto. Analisa como essa abordagem é apresentada e debatida na consulta pública do CGI.br e na audiência pública do STF sobre a constitucionalidade do art. 19 do Marco Civil da Internet. Os resultados demonstram o estado incipiente do debate sobre o dever de cuidado em plataformas e a importância de um processo regulatório para plataformas digitais que equilibre a liberdade de expressão com a prevenção de danos e a proteção do usuário.

### **Ataques à democracia no Brasil, uma análise da repercussão do 8 de janeiro**

(Rita Paulino, Ivone Rocha, Adriano Madureira, Marcos Seruffo)

Apresenta uma pesquisa realizada na rede social X (ex-Twitter) que investiga a repercussão, por esse canal, dos atos de invasão no Congresso Nacional, Supremo Tribunal Federal (STF) e Palácio do Planalto, em Brasília (DF), no dia 8 de janeiro de 2023. O estudo relata métodos digitais diferenciados para entender o contexto do fato investigado desde a coleta de dados com os termos emblemáticos que foram mais divulgados durante as coberturas jornalísticas no Brasil.

Esta edição também inclui um relato minucioso do professor Charles Mok, de Stanford, sobre o surgimento do DeepSeek -- o sistema de inteligência artificial (IA) em código aberto originário da China que causou um terremoto (técnico e econômico) no espaço de desenvolvimento dos chamados "large language models" (LLMs), uma nova etapa do avanço dos sistemas de inteligência artificial. O artigo foi escrito no início de 2025. Desde então, o avanço do DeepSeek (e dos outros sistemas similares) tem sido excepcional e abrangendo cada vez mais todos os campos de conhecimento, mas o texto do professor Mok é referência essencial para entender como se deu esse processo.

Desde o início de 2025, o DeepSeek tem sido o foco de atenção dentro e fora da comunidade de IA. Comparações entre ele e outros LLMs hoje populares (como Claude, Gemini, GPT e Llama) mostram que esta variante dos LLMs está basicamente à altura de todos os outros. DeepSeek demonstrou precisão superior à do ChatGPT e Gemini na resolução de complexos problemas matemáticos<sup>1</sup>. No campo da criação de software, utilizando uma das linguagens mais adotadas na programação Web, o DeepSeek demonstrou "maior precisão na geração de código Python, frequentemente exigindo menos tentativas, o que sugere uma vantagem na resolução algorítmica de problemas<sup>2</sup>."

DeepSeek é hoje usado em aplicações em saúde, educação, produção de software, resolução de problemas matemáticos, aplicações em mídia etc, tal como outros chatbots. O impacto maior, no momento, é o fato de o software ser de código aberto e sem custo significativo para o usuário, o que desequilibra e põe em grave risco o modelo de negócios dos LLMs, com rumores fortes de colapso de mais uma bolha, remanescente da crise das "dot.com" no ano 2000.

Cabe aqui uma digressão sobre os conceitos de inteligência artificial (IA), modelos de linguagem, e a dicotomia entre linguagem e percepção humana. Citando uma contribuição de vários autores liderados por Dan Hendricks na definição da IA:

*"A Inteligência Artificial Geral (IAG) é uma IA que pode igualar ou superar a versatilidade e a proficiência cognitiva de um adulto bem-educado. Essa definição enfatiza que a inteligência geral requer não apenas desempenho especializado em domínios específicos, mas a amplitude (versatilidade) e a profundidade (proficiência) de habilidades que caracterizam a cognição humana. Para operacionalizar essa definição, devemos observar o único exemplo existente de inteligência geral: os humanos. A cognição humana não é uma capacidade monolítica; é uma arquitetura complexa composta por muitas habilidades distintas aprimoradas pela evolução. Essas habilidades possibilitam nossa notável adaptabilidade<sup>3</sup>."*

Como destaca Benjamin Riley, uma característica comum aos chatbots é que são modelos de linguagem, baseados na coleta maciça de dados linguísticos, organizados em palavras ou partes de palavras denominadas "tokens", e na busca de correlações entre elas a partir de comandos de consulta. Humanos usam um idioma para comunicar os resultados de nossa capacidade de raciocinar, formar abstrações

---

1. Tianchen Gao et al, "A Comparison of DeepSeek and Other LLMs", arXiv:2502.03688v2 [cs.CL] 26 Feb 2025.  
2. Md Motaleb Hossen Manik, "ChatGPT vs. DeepSeek: A Comparative Study on AI-Based Code Generation", Department of Computer Science, Rensselaer Polytechnic Institute (RPI), n/d.  
3. Dan Hendricks et al., "A Definition of Artificial General Intelligence", <https://arxiv.org/abs/2510.18212v3>

e produzir generalizações -- o que definimos como nossa inteligência. O idioma é um instrumento para expressar nossa capacidade de pensar. Em síntese, diz Riley:

*"Os LLMs são simplesmente ferramentas que emulam a função comunicativa da linguagem, não o processo cognitivo separado e distinto de pensar e raciocinar, independentemente de quantos datacentros construímos. Usamos a linguagem para pensar, mas isso não faz da linguagem o mesmo que pensamento."*<sup>4</sup>

Assim, os LLMs estão longe de cobrir a amplitude, dinâmica e diversidade da inteligência humana. No atual paradigma dos LLMs, jamais cobrirão.

A edição também inclui uma minuciosa análise do Dr Wolfgang Kleinwächter (publicada originalmente em inglês na revista online CircleID<sup>5</sup>) sobre o processo e os resultados sintetizados no documento final do encontro de avaliação de 20 anos da Cúpula Mundial sobre a Sociedade da Informação, em dezembro de 2025 (CMSI+20/WSIS+20), incluindo o Fórum de Governança da Internet (FGI/IGF).

Os 20 anos desde o primeiro FGI não tinham estabelecido alguns critérios fundamentais para sua continuidade e eventual aprofundamento. Mantido ao longo de todo esse período de duas décadas como um evento não permanente e sem garantias de financiamento de sua estrutura administrativa básica, o FGI entretando estimulou a criação de dezenas de processos nacionais e regionais de discussão sobre a governança da Internet.

Em 2025 eram contabilizados mais de 180 fóruns nacionais e regionais de governança da Internet (NRIs) ativos em todo o mundo. O secretariado do FGI reconhecia, em abril de 2025, mais de 176 iniciativas nas cinco regiões da ONU. Esses fóruns fornecem perspectivas locais e regionais cruciais para o diálogo global sobre governança da Internet, operando de forma independente, mas de acordo com os princípios fundamentais do FGI de serem multissetoriais, abertos e participativos. Essa teia internacional de iniciativas é uma das principais razões que justifica a permanência do FGI.

Boa leitura :-)

---

4. Benjamin Riley, "Large language mistake", 25-11-2025, em <https://www.theverge.com/ai-artificial-intelligence/827820/large-language-models-ai-intelligence-neuroscience-problems>.

5. <https://circleid.com/posts/wsis20-a-small-light-of-hope-in-a-darkening-political-landscape>



[ índice ]

01 EDUCAÇÃO E CAPACITAÇÃO PARA REGULAÇÃO DIGITAL: O PAPEL DAS INSTITUIÇÕES  
NA FORMAÇÃO DE ESPECIALISTAS  
Rodrigo Moreira dos Santos

12 TRANSPARÊNCIA DE DADOS EM CONTEÚDOS DE INTERESSE PÚBLICO:  
PROPOSTAS DE REGULAÇÃO PARA PLATAFORMAS DIGITAIS NO BRASIL  
Eliandro Jeovane Natal da Silva

30 MÍDIAS SOCIAIS, REGULAÇÃO PROCESSUAL E DEVER DE  
CUIDADO: EVIDÊNCIAS EMPÍRICAS DO DEBATE NO BRASIL  
Ivar Hartmann  
Ramon Costa  
Bruno Oliveira

44 ATAQUES À DEMOCRACIA NO BRASIL, UMA ANÁLISE DA REPERCUSSÃO DO 8 DE JANEIRO  
Rita Paulino  
Ivone Rocha  
Adriano Madureira  
Marcos Seruffo

58 UM BALANÇO DO CHOQUE DO DEEPSEEK  
CHARLES MOK

76 CMSI+20/WSIS+20: UMA PEQUENA LUZ DE ESPERANÇA EM UM  
CENÁRIO POLÍTICO CADA VEZ MAIS SOMBRIO  
Wolfgang Kleinwächter



# EDUCAÇÃO E CAPACITAÇÃO PARA REGULACÃO DIGITAL

O papel das instituições na formação de especialistas

Rodrigo Moreira dos Santos

## Resumo

A era digital trouxe novos desafios à governança e à proteção de dados, exigindo ações integradas para garantir que a tecnologia seja usada de maneira ética e transparente. Este estudo, fundamentado nos dados da consulta pública do CGI.br sobre regulação de plataformas digitais, investiga as lacunas na capacitação profissional e apresenta propostas práticas para fortalecer a regulação digital no Brasil. A pesquisa destaca a necessidade de currículos interdisciplinares que integrem tecnologia, direito e ética, bem como programas de certificação e parcerias público-privadas para expandir o acesso ao

conhecimento especializado. Inspirado em modelos internacionais como o GDPR, na União Europeia, e os frameworks do NIST, nos Estados Unidos, o trabalho explora como essas experiências podem ser adaptadas à realidade brasileira, promovendo soberania digital e reduzindo a dependência de tecnologias estrangeiras. Conclui-se que a capacitação profissional é essencial não apenas para atender às exigências legais, mas para construir um mercado mais ético e competitivo, proteger os direitos dos cidadãos e posicionar o Brasil como líder em regulação digital na América Latina.

## Introdução

A transformação digital está remodelando os pilares que sustentam a sociedade moderna, afetando de maneira profunda as relações econômicas, sociais e políticas. As plataformas digitais, protagonistas desse processo, oferecem benefícios significativos, como inovação tecnológica, novas oportunidades de negócios e maior conectividade global. No entanto, essas mesmas plataformas trazem consigo desafios críticos que afetam diretamente a privacidade, a segurança e a soberania dos dados pessoais. O Brasil, com a implementação da Lei Geral de Proteção

de Dados (LGPD), deu um importante passo para estabelecer diretrizes de proteção e governança digital, mas enfrenta barreiras estruturais e educacionais que dificultam a aplicação eficaz dessa legislação em um cenário de rápida evolução tecnológica.

Este estudo, baseado nas contribuições da consulta pública do CGI.br sobre regulação de plataformas digitais, revela lacunas substanciais na formação de profissionais capazes de implementar e monitorar regulações digitais de forma eficiente. As conclusões da pesquisa destacam a ausência

de currículos interdisciplinares que integrem tecnologia, direito e ética, e apontam para a necessidade de programas de certificação e parcerias público-privadas como caminhos essenciais para capacitação. Ao mesmo tempo, modelos internacionais, como o GDPR, na União Europeia, e os frameworks do NIST, nos Estados Unidos, oferecem exemplos inspiradores de como unir

## Metodologia

Este estudo fundamenta-se nos dados obtidos pela consulta pública promovida pelo Comitê Gestor da Internet no Brasil (CGI.br) em 2023. A consulta reuniu contribuições de quatro setores principais – governamental, empresarial, terceiro setor e comunidade científica – sobre a regulação de plataformas digitais. O objetivo principal desta análise foi identificar as principais lacunas e demandas relacionadas à capacitação profissional e propor soluções con-

regulação e educação para construir um ambiente digital mais ético e transparente. Este artigo busca não apenas explorar essas referências, mas adaptá-las à realidade brasileira, propondo ações estratégicas para que o país consolide sua soberania digital, proteja os direitos dos cidadãos e fortaleça sua posição como líder em regulação digital na América Latina.

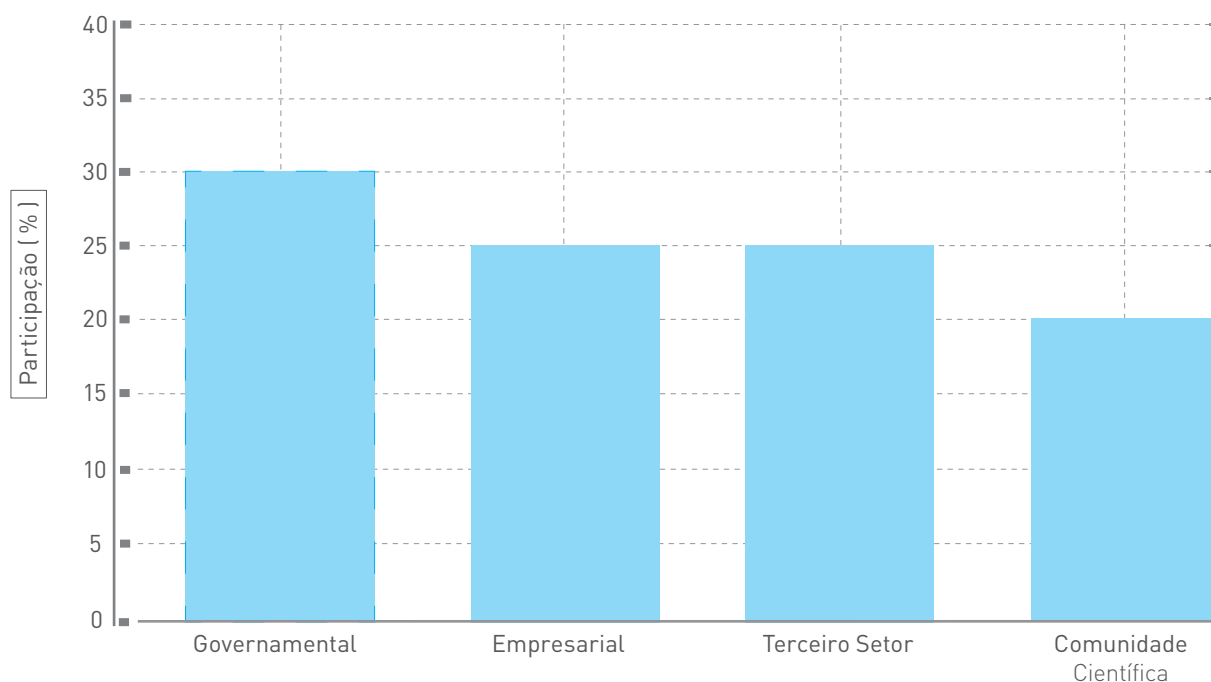
cretas para fortalecer a regulação digital no Brasil.

### COLETA E ORGANIZAÇÃO DOS DADOS

Os dados, disponibilizados nos formatos CSV e JSON, foram acessados no portal oficial do CGI.br. Após o download, as contribuições foram organizadas e preparadas para análise. O conjunto passou por uma etapa de limpeza para eliminar entradas duplicadas e irrelevantes, garantindo a qualidade das informações utilizadas.

### GRÁFICO 1: PARTICIPAÇÃO POR SETOR NA CONSULTA PÚBLICA

Para contextualizar a origem das contribuições, o gráfico abaixo ilustra a participação relativa dos setores na consulta pública:



## Classificação Temática

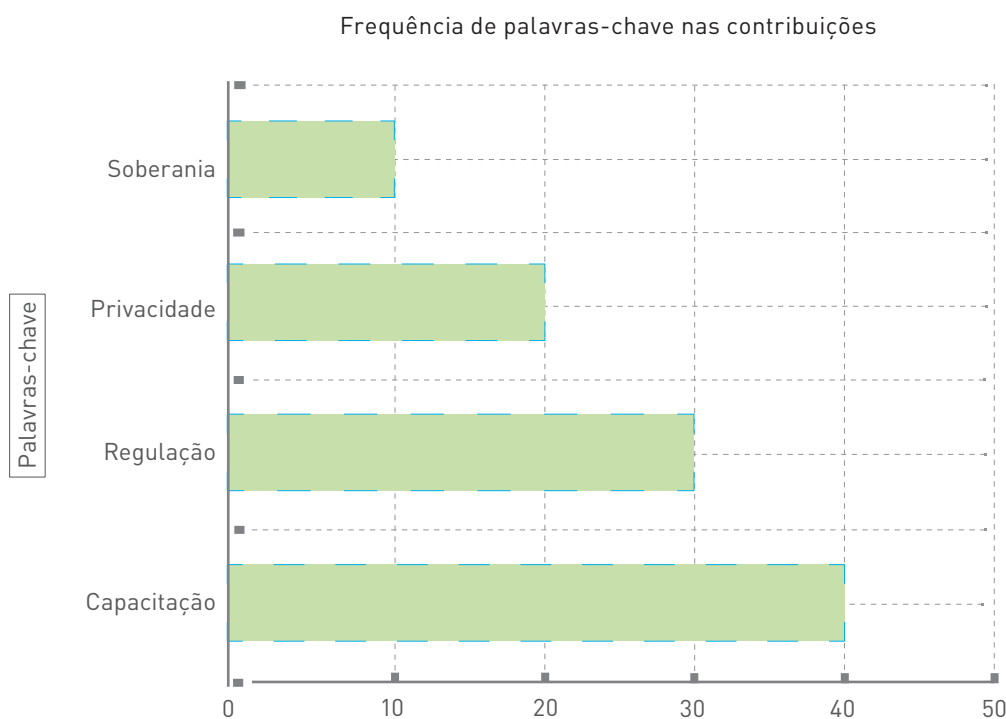
A análise das contribuições baseou-se na identificação de categorias principais, como:

- Lacunas na capacitação profissional.
- Propostas para desenvolvimento de currículos interdisciplinares.
- Demandas por parcerias público-privadas.
- Sugestões para proteção de dados e soberania digital.

Essas categorias foram escolhidas com base na relevância para o tema do artigo e na frequência das menções nas contribuições. Cada uma foi subdividida em subcategorias específicas, como auditoria de compliance, privacidade infantil e transparência.

### GRÁFICO 2: DISTRIBUIÇÃO DAS CONTRIBUIÇÕES POR CATEGORIA

A distribuição das contribuições entre as categorias identificadas está representada no gráfico a seguir:



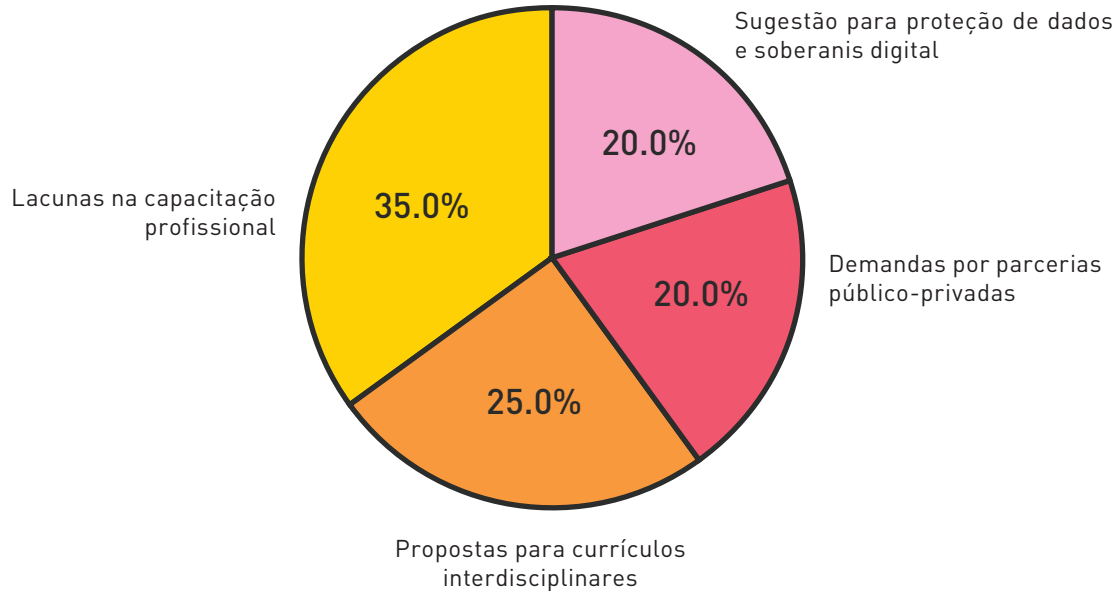
## Análise Qualitativa e Quantitativa

Após a categorização, foi realizada uma análise qualitativa para identificar padrões e tendências nas contribuições. Palavras-chave como **"capacitação"**, **"regulação"** e **"privacidade"** foram

utilizadas para guiar essa etapa. Além disso, uma análise quantitativa mediu a frequência de termos nas categorias, permitindo um mapeamento das prioridades da sociedade.

### GRÁFICO 3: FREQUÊNCIA DE PALAVRAS-CHAVE NAS CONTRIBUIÇÕES

Abaixo, apresentamos a frequência dos termos mais mencionados pelos participantes da consulta:



## Cruzamento com Modelos Internacionais

Para enriquecer a análise, foram revisadas práticas internacionais bem-sucedidas, como:

- O Regulamento Geral de Proteção de Dados (GDPR) na União Europeia, com foco em treinamentos voltados à privacidade e compliance.
- Frameworks do NIST nos Estados Unidos, que promovem educação e treinamento para segurança e governança digital.

### SÍNTESE E INTERPRETAÇÃO DOS RESULTADOS

Os dados analisados foram sintetizados em tabelas e gráficos para facilitar a interpretação. Essas visualizações embasaram as discussões e propostas apresentadas ao longo do artigo.

## Discussão

A análise das contribuições recebidas na consulta pública do CGI.br revelou um panorama detalhado sobre os desafios e oportunidades relacionados à capacitação profissional em regulação digital no Brasil. Esta seção explora as lacunas identificadas, apresenta propostas concretas e discute como esses achados podem contribuir para a construção de um ecossistema regulatório

eficiente, ético e alinhado às demandas da sociedade brasileira.

### Lacunas na Capacitação Profissional

Um dos pontos mais destacados nas contribuições foi a insuficiência de programas específicos voltados à formação de especialistas em regulação digital. Muitos participantes apontaram que o sistema

educacional brasileiro, em geral, não aborda temas como proteção de dados, auditoria de compliance e governança digital de maneira estruturada. Essa lacuna impacta diretamente a aplicação de legislações como a LGPD e enfraquece a capacidade do país de responder aos desafios impostos pela rápida evolução tecnológica. Além disso, foi identificado que a formação disponível atualmente é altamente segmentada, com profissionais de tecnologia recebendo pouca ou nenhuma instrução sobre aspectos legais e éticos, enquanto especialistas em direito muitas vezes carecem de entendimento técnico sobre as operações de plataformas digitais. Essa desconexão dificulta uma abordagem integrada e colaborativa na aplicação das normas regulatórias.

## Propostas Baseadas nas Contribuições

### 1. DESENVOLVIMENTO DE CURRÍCULOS INTERDISCIPLINARES

A construção de currículos interdisciplinares é uma das propostas mais relevantes para enfrentar as lacunas identificadas na capacitação profissional em regulação digital. Esses currículos devem transcender as abordagens tradicionais, integrando disciplinas de tecnologia, direito, ética e governança digital. A ideia é preparar profissionais com uma visão holística, capazes de compreender não apenas os aspectos técnicos das plataformas digitais, mas também as implicações legais e éticas associadas. Ao incluir fundamentos de proteção de dados e privacidade, esses programas educacionais oferecem aos alunos uma base sólida para entender a importância da LGPD e outras regulamentações globais, como o GDPR. Além disso, a introdução de análises de risco e auditorias de compliance como componentes centrais do currículo

Um dos pontos mais destacados nas contribuições foi a insuficiência de programas específicos voltados à formação de especialistas em regulação digital. Muitos participantes apontaram que o sistema educacional brasileiro, em geral, não aborda temas como proteção de dados, auditoria de compliance e governança digital de maneira estruturada.

capacita os futuros especialistas a identificar falhas e propor soluções eficazes em um ambiente de rápida evolução tecnológica. Estudos de caso são outro elemento essencial. Ao explorar situações reais de aplicação da LGPD e outras legislações, os alunos podem visualizar os desafios e as complexidades do mundo real. Essa abordagem prática não apenas enriquece o aprendizado, mas também promove uma capacidade crítica e inovadora de pensar soluções que antecipem desafios futuros. Finalmente, o uso de ferramentas tecnológicas, como plataformas

de monitoramento e controle de dados, prepara os alunos para atuar diretamente no mercado. Aprender a utilizar essas tecnologias durante a formação acadêmica reduz a curva de aprendizado nas empresas e fortalece o alinhamento entre os profissionais e as demandas do setor.

## **2. PARCERIAS PÚBLICO-PRIVADAS**

A colaboração entre universidades, órgãos governamentais e empresas de tecnologia é um elemento central para o fortalecimento da capacitação em regulação digital no Brasil. Parcerias público-privadas (PPPs) oferecem uma oportunidade única de unir expertise prática e recursos financeiros do setor privado com a missão educativa e inclusiva das instituições públicas. Essa sinergia pode acelerar a formação de profissionais qualificados e criar soluções adaptadas às demandas específicas do mercado e da sociedade. Por meio dessas parcerias, programas especializados de treinamento podem ser financiados e desenvolvidos, garantindo acesso a recursos de última geração e a metodologias avançadas de ensino. As empresas de tecnologia, por exemplo, podem contribuir com cases reais de auditorias e conformidade, enquanto os órgãos governamentais oferecem o contexto regulatório necessário para preparar os alunos para desafios práticos. Além disso, as PPPs podem fomentar estágios e experiências práticas, inserindo os futuros especialistas em cenários reais de aplicação, onde possam atuar diretamente no monitoramento, controle e auditoria de plataformas digitais. Outro benefício importante dessas parcerias é a possibilidade de criar ferramentas educacionais baseadas em casos concretos. Plataformas simuladas que replicam ambientes de regulação, como auditorias virtuais de plataformas digitais, permitem que os alunos vivenciem situações

reais de trabalho em um ambiente controlado. Essas simulações não apenas melhoram o aprendizado, mas também garantem que os profissionais entrem no mercado com experiência prática relevante. Mais do que uma iniciativa educativa, as parcerias público-privadas têm o potencial de criar um ciclo virtuoso. O setor privado, ao compartilhar suas melhores práticas, contribui para a formação de profissionais mais capacitados, enquanto as instituições públicas garantem que esses programas sejam acessíveis e alinhados aos interesses coletivos. Essa abordagem inclusiva amplia o alcance da capacitação, permitindo que profissionais de diferentes regiões e contextos socioeconômicos tenham acesso a oportunidades de qualificação e desenvolvimento.

## **3. PROGRAMAS DE CERTIFICAÇÃO**

A criação de programas de certificação nacionais é uma estratégia essencial para preencher as lacunas de capacitação em regulação digital no Brasil. Certificações específicas não apenas estabelecem padrões claros de excelência, mas também garantem que os profissionais estejam preparados para atender às demandas do mercado e às exigências legais, como a implementação da LGPD. Essas certificações são especialmente relevantes em um cenário onde a qualificação técnica e prática é fundamental para lidar com as complexidades das plataformas digitais.

Certificações nacionais podem ser projetadas para atender diferentes níveis de experiência e complexidade. Profissionais em início de carreira podem acessar módulos básicos que introduzem conceitos de proteção de dados, auditoria de compliance e governança digital. Já para especialistas mais experientes, os programas podem incluir tópicos avançados, como privacidade infantil, transparência e auditorias aprofundadas. Essa estrutura progressiva cria um pipeline

de desenvolvimento profissional que beneficia tanto os indivíduos quanto as organizações que os empregam. Além disso, certificações específicas para setores ou temáticas prioritárias, como transparência no uso de dados e segurança em plataformas voltadas para crianças, foram amplamente sugeridas nas contribuições da consulta pública.

Esses programas ajudam a atender demandas específicas do mercado e alinham os profissionais às necessidades de áreas críticas. Ao integrar certificações reconhecidas tanto pelo governo quanto pelo setor privado, o Brasil pode criar um sistema padronizado que valorize a qualificação e promova a confiança nas competências dos profissionais certificados. O impacto das certificações vai além da qualificação

técnica. Elas reforçam a credibilidade dos profissionais e das empresas que contratam seus serviços, promovendo uma cultura de responsabilidade digital e conformidade. No longo prazo, essas iniciativas podem aumentar a competitividade do mercado brasileiro, criando profissionais capazes de se destacar globalmente e atrair investimentos internacionais em tecnologia e regulação. Ao estabelecer certificações como um pilar central da capacitação em regulação digital, o Brasil não apenas responde às demandas regulatórias atuais, mas também se posiciona estrategicamente para enfrentar os desafios futuros da era digital. Essa abordagem cria uma base sólida para a construção de um ecossistema tecnológico mais ético, inovador e alinhado com os direitos dos cidadãos.

---

## Modelos Internacionais Inspiradores

A experiência internacional oferece valiosas lições para o desenvolvimento de uma estratégia robusta de capacitação em regulação digital no Brasil. Modelos como o Regulamento Geral de Proteção de Dados (GDPR), na União Europeia, e os *frameworks* do *National Institute of Standards and Technology* (NIST), nos Estados Unidos, são exemplos de como políticas bem estruturadas, associadas a programas de formação, podem promover avanços significativos em governança digital.

O GDPR, implementado em 2018, tornou-se uma referência global para proteção de dados e privacidade. Além de estabelecer um marco regulatório rigoroso, impulsionou a criação de uma ampla rede de treinamentos e certificações voltadas para compliance. Universidades e instituições na Europa integram o GDPR em currículos interdisciplinares, oferecendo cursos que combinam teoria e prática. Treinamentos modulares são ajustados para diferentes

setores econômicos, permitindo que empresas e profissionais desenvolvam competências específicas para atender às exigências regulatórias. Ferramentas práticas de auditoria de compliance, baseadas nos princípios do GDPR, também têm sido amplamente utilizadas, fortalecendo a capacidade de supervisão e governança de dados.

Nos Estados Unidos, o NIST promove *frameworks* reconhecidos mundialmente, como o *Cybersecurity Framework*, que fornece diretrizes claras para gerenciar riscos digitais e implementar boas práticas de segurança. O NIST também desenvolve programas de capacitação acessíveis, incluindo workshops e materiais educativos que abrangem desde fundamentos de segurança cibernética até a governança de privacidade. Essa abordagem prática e acessível democratiza o conhecimento técnico, permitindo que organizações de diferentes portes implementem políticas

robustas de regulação e proteção de dados.

Embora os contextos europeu e norte-americano apresentem diferenças culturais e regulatórias em relação ao Brasil, ambos oferecem elementos que podem ser adaptados à realidade brasileira. O desenvolvimento de currículos interdisciplinares, inspirado pelo GDPR, e a criação de frameworks acessíveis e aplicáveis, como os do NIST, são estratégias viáveis para enfrentar os desafios

da capacitação em regulação digital no Brasil. Esses modelos internacionais destacam a importância de combinar regulação e capacitação como pilares complementares. Ao integrar as melhores práticas globais com as demandas específicas do Brasil, é possível construir uma base educacional e regulatória que fortaleça a governança digital, proteja os direitos dos cidadãos e promova a soberania tecnológica do país.

---

## Oportunidades e Desafios para o Brasil

O cenário brasileiro apresenta características únicas que demandam adaptações cuidadosas das práticas internacionais para maximizar o impacto das iniciativas de capacitação em regulação digital. Embora o país tenha avançado na implementação de legislações como a LGPD, a efetividade dessa regulação depende da superação de desafios estruturais e da exploração de oportunidades específicas que podem posicionar o Brasil como líder regional e global em governança digital. Uma das principais oportunidades está na acessibilidade dos programas educacionais. Ao integrar tecnologia em currículos e utilizar plataformas digitais para ensino a distância, é possível expandir o alcance da capacitação para regiões remotas e populações historicamente excluídas do acesso a uma educação de qualidade.

Essa abordagem não apenas reduz desigualdades regionais, mas também cria um mercado de trabalho mais diversificado, onde profissionais de diferentes contextos podem contribuir de maneira significativa para a regulação digital. Outro aspecto crucial é o potencial do Brasil para liderar a regulação digital na América Latina. A construção de parcerias regionais pode promover o intercâmbio de conhecimento

e a padronização de práticas regulatórias, fortalecendo a posição do país como referência na proteção de dados e no desenvolvimento de soluções locais.

Essa liderança regional é fundamental para enfrentar desafios compartilhados, como a dependência de tecnologias estrangeiras e a vulnerabilidade a infraestruturas críticas controladas por empresas internacionais. Entretanto, a soberania digital é um dos maiores desafios enfrentados pelo Brasil. A forte dependência de plataformas e tecnologias estrangeiras limita a autonomia nacional e aumenta os riscos de exposição a legislações e interesses externos. Para enfrentar essa questão, é essencial incentivar a pesquisa e o desenvolvimento de soluções tecnológicas locais, promovendo a criação de ferramentas e plataformas adaptadas às necessidades brasileiras. O investimento em inovação e a criação de ecossistemas tecnológicos autossuficientes são passos fundamentais para garantir a independência tecnológica do país.

Além disso, a falta de integração entre academia, setor público e setor privado continua sendo um obstáculo para o progresso em regulação digital. É necessário criar um ambiente colaborativo onde universidades desenvolvam currículos alinhados às

demandas do mercado, o governo atue como facilitador e regulador, e as empresas contribuam com expertise prática. Essa sinergia pode acelerar o desenvolvimento de soluções eficazes para os desafios regulatórios e garantir que a capacitação atenda às necessidades atuais e futuras. Por fim, o Brasil enfrenta o desafio de preparar-se para questões emergentes, como o impacto da inteligência artificial, a desinformação e o avanço de tecnologias descentralizadas. Essas novas dinâmicas demandam uma abordagem educacional e regulatória flexível, que não apenas reaja às mudanças, mas também antecipe tendências e inovações. O país tem a oportunidade de construir um modelo de regulação digital que não apenas atenda às suas necessidades internas, mas também sirva como referência para outras nações em busca de equilíbrio entre tecnologia, ética e governança. Ao combinar inovação, inclusão e soberania, o Brasil pode transformar esses desafios em oportunidades para liderar a era digital com responsabilidade e visão estratégica. Essa abordagem cria as bases para um futuro onde a tecnologia seja utilizada de forma ética, sustentável e alinhada aos interesses da sociedade.

### **IMPACTO ESPERADO**

A implementação das propostas apresentadas neste artigo promete transformar significativamente o cenário da regulação digital no Brasil. Ao priorizar a capacitação profissional e a construção de um ecossistema regulatório robusto, o país pode consolidar um modelo de governança digital eficiente, ético e inclusivo. Um impacto central é o fortalecimento da confiança da sociedade nas plataformas digitais e nos mecanismos de proteção de dados.

Profissionais mais qualificados, alinhados às exigências da LGPD, permitirão práticas de coleta e uso de informações pessoais

mais transparentes e seguras. Isso garante que os cidadãos sintam-se protegidos e empoderados em suas interações digitais, enquanto as empresas, ao cumprirem as normas com rigor, conquistam credibilidade em um mercado competitivo e cada vez mais exigente. A qualificação técnica também impulsiona a criação de um mercado mais ético e equilibrado.

Por meio de programas de certificação e parcerias público-privadas, pequenos negócios e grandes corporações terão acesso igualitário a treinamentos e ferramentas que lhes permitam implementar práticas de compliance de maneira eficaz. Além disso, a presença de profissionais devidamente capacitados aumenta a atratividade do Brasil para investidores estrangeiros, consolidando o país como um centro de excelência na regulação digital na América Latina. No campo educacional, a inclusão de disciplinas interdisciplinares nas universidades, combinada com a oferta de programas de ensino a distância e treinamentos acessíveis, expande o alcance da capacitação para regiões e grupos que historicamente tiveram menos acesso a oportunidades de qualificação.

Isso contribui para a redução de desigualdades regionais e socioeconômicas, diversificando o mercado de trabalho e fortalecendo setores críticos da economia digital. Outro efeito estratégico das propostas é o fortalecimento da soberania digital do Brasil. O incentivo ao desenvolvimento de tecnologias nacionais e a redução da dependência de plataformas estrangeiras criam um ambiente de maior autonomia tecnológica.

Com isso, o país fortalece sua infraestrutura crítica e se posiciona como um líder global em regulação digital, capaz de moldar padrões regionais na América Latina. Além disso, o Brasil estará mais bem preparado para enfrentar desafios futuros, como a governança da inteligência artificial,

o combate à desinformação e a regulação de tecnologias emergentes. A capacitação contínua de profissionais especializados permitirá que o país antecipe tendências e lide com mudanças tecnológicas de forma proativa, garantindo que a evolução digital esteja sempre alinhada à proteção dos direitos dos cidadãos e à promoção da ética no uso da tecnologia.

Ao investir em capacitação e regulação digital, o Brasil não apenas atende às demandas atuais, mas cria as condições para um futuro onde a inclusão, a transparência e o respeito aos direitos individuais sejam prioridades. O impacto esperado é um país mais autônomo e competitivo, capaz de liderar a era digital com responsabilidade e visão estratégica, colocando a proteção e o bem-estar dos cidadãos no centro de sua governança tecnológica.

## Conclusão

Um dos grandes desafios da era digital é a regulação das plataformas digitais, exigindo ações coordenadas que alinhem tecnologia, ética e proteção de direitos. Este estudo, com base nos dados da consulta pública do CGI.br, evidenciou que a capacitação profissional é o pilar indispensável para alcançar uma governança digital eficiente no Brasil. A formação interdisciplinar,

combinando tecnologia, direito e ética, e a implementação de programas de certificação e parcerias público-privadas emergem como estratégias cruciais para suprir lacunas identificadas e promover um ambiente regulatório robusto e inclusivo. Além disso, o incentivo à pesquisa e ao desenvolvimento de tecnologias locais é essencial para reduzir a dependência de soluções estrangeiras e fortalecer a soberania digital do país.

Ao investir em capacitação, o Brasil não apenas atende às demandas da LGPD, mas também cria condições para um mercado mais ético, competitivo e alinhado às necessidades dos cidadãos. A implementação das propostas discutidas – incluindo currículos inovadores, certificações e parcerias estratégicas – permite que o país enfrente com eficácia desafios emergentes, como a inteligência artificial e a desinformação, enquanto protege os direitos dos indivíduos e garante transparência nas práticas digitais. Com ações decisivas e coordenadas, o Brasil tem a oportunidade de transformar os desafios da era digital em um modelo de governança que coloca a inclusão, a soberania e o bem-estar coletivo no centro de sua estratégia, posicionando-se como líder global em regulação digital. ■

**Rodrigo Moreira dos Santos** é professor universitário e consultor em Tecnologia da Informação, com mais de 25 anos de experiência em ensino, pesquisa e projetos de inovação digital. Atua nas áreas de Cibersegurança, Inteligência Artificial, Ciência de Dados e Governança Digital, lecionando em instituições como UniFECAP e Jala University. É graduado em Sistemas de Informação e pós-graduado em Tecnologia da Informação Aplicada à Educação, Desenvolvimento Blockchain, Big Data e Business Intelligence, com foco em tornar a tecnologia acessível a todos, promovendo uma formação prática e eticamente responsável.

## Referências

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n.º 13.709, de 14 de agosto de 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm). Acesso em: 25 nov. 2024.

CGI.br. Consulta Pública sobre Regulação de Plataformas Digitais. 2023. Disponível em: <https://dialogos.cgi.br/documentos/debate/consulta-plataformas/>. Acesso em: 25 nov. 2024.

EUROPEAN UNION. General Data Protection Regulation (GDPR). 2018. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 25 nov. 2024.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Cybersecurity Framework. Disponível em: <https://www.nist.gov/cyberframework>. Acesso em: 25 nov. 2024.

NIC.br. Relatório de Sistematização da Consulta Pública sobre Regulação de Plataformas Digitais. São Paulo: CGI.br, 2023. Disponível em: <https://dialogos.cgi.br/documentos/debate/consulta-plataformas/>. Acesso em: 25 nov. 2024.

SILVA, Fábio. Capacitação e Governança Digital no Brasil: uma análise das lacunas e oportunidades na formação de especialistas. Revista Brasileira de Governança Digital, v. 5, n. 2, p. 45-60, 2023.



# Transparência de dados

em conteúdos de interesse público

Propostas de regulação para plataformas digitais no Brasil

Eliandro Jeovane Natal da Silva

## Resumo

O crescimento das plataformas digitais apresenta desafios relacionados à privacidade, transparência e governança ética. O presente artigo explora a necessidade de maior transparência de dados em conteúdos de interesse público nas plataformas digitais, regulamentações mais claras e rigorosas sobre o uso de dados pessoais, e a moderação de conteúdo. Foi utilizada a consulta pública do Comitê Gestor da Internet no Brasil (CGI.br), em 2023, para propor soluções concretas e alinhadas aos direitos dos usuários e à inovação digital. Discute-se a necessidade de medidas adicionais para garantir a pluralidade de informações, a

proteção de dados pessoais, a transparência nos processos de moderação e pela criação de autoridades regulatórias independentes para fiscalizar o cumprimento das normas e aplicar sanções justas, promovendo um ambiente digital mais equitativo. Com base na análise das contribuições da consulta pública do CGI.br (2023), propõe-se a implementação de uma governança mais robusta e transparente. Esta governança deve incluir regulações precisas e rigorosas sobre o uso de dados pessoais e a moderação de conteúdo, assegurando o equilíbrio entre interesses comerciais e a proteção dos direitos fundamentais dos usuários.

## Introdução

Com o avanço acelerado da tecnologia e a popularização da Internet nas últimas décadas, as plataformas digitais têm desempenhado um papel central na disseminação de informações, na comunicação social e na vida cotidiana das pessoas. Com este alcance e influência, as práticas adotadas por estas plataformas em relação ao uso de dados pessoais e à moderação de conteúdo tornaram-se temas de grande relevância, especialmente no que diz respeito a transparência dessas ações. A coleta e o uso de dados pessoais, por exemplo, frequentemente envolvem políticas complexas e pouco acessíveis, dificultando a compreensão dos usuários e comprometendo o consentimento informado (Tufekci, 2014).

A falta de transparência nas práticas de

moderação de conteúdo e a ausência de mecanismos compreensíveis de governança trazem desafios significativos, como a manipulação de informações, a amplificação da desinformação e a promoção de práticas antiéticas na comunicação digital. Estas questões impactam diretamente à privacidade, à autonomia e à segurança dos usuários (Acquisti; Gross; Stutzman, 2016).

Nesse contexto, o Comitê Gestor da Internet no Brasil (CGI.br)<sup>1</sup> e a Revista PoliTICs<sup>2</sup> lançaram uma chamada para artigos científicos que contribuam ao debate sobre a regulação de plataformas digitais no Brasil. Este artigo insere-se nesta iniciativa ao focalizar na análise das perguntas e respostas da consulta pública realizada pelo CGI.br no ano de 2023.

1. Comitê Gestor da Internet no Brasil. Sobre o CGI.br. Disponível em: <https://www.cgi.br>. Acesso em: 12 nov. 2024.

2. poliTICs: revista de estudos sobre governança, Internet e tecnologia. Disponível em: <https://politics.org.br>. Acesso em: 01 nov. 2024

## Metodologia

Este estudo adota uma metodologia estruturada e fundamentada em múltiplos componentes, alinhada às recomendações de autores como Triviños (1987), Lakatos e Marconi (1992), e Yin (1992). A pesquisa é

classificada como bibliográfica e documental, com base na análise sistemática de documentos oficiais, artigos acadêmicos e outras fontes documentais, além de contribuições da consulta pública organizada pelo CGI.

**Quadro 1 – Desenho metodológico**

COMPONENTES DA METODOLOGIA	CARACTERÍSTICAS DO ESTUDO	ETAPAS DO ARTIGO
Tipo de estudo	Bibliográfico e documental	Análise de documentos, artigos, leis e consulta pública do CGI.br.
Enfoque da pesquisa	Qualitativo	Estudo de caso da Pergunta 31-V da consulta pública do CGI.br.

Fonte: Os autores (2024).

O enfoque da pesquisa é qualitativo e inclui a análise da Pergunta 31-V da consulta pública promovida pelo CGI.br [2023], que aborda “categorias de conteúdos de claro interesse público que sejam submetidas a mecanismos mais rigorosos de transparência”. Esta pergunta foi selecionada por sua relevância para compreender as demandas sociais e as possibilidades de regulamentação que promovam maior transparência no gerenciamento de dados e moderação de conteúdo pelas plataformas digitais.

A partir da análise das respostas à Pergunta 31-V da consulta pública promovida pelo CGI.br, é possível identificar categorias de conteúdos que, por seu evidente interesse público, demandam maior rigor na aplicação de mecanismos de transparência. Entre essas categorias, destacam-se:

- Períodos eleitorais, apontado pela contribuição do Instituto Vero.
- Defesa de direitos de crianças e adolescentes, apontado pela contribuição do Instituto Alana<sup>3</sup>.

### Transparência de dados em períodos eleitorais nas plataformas digitais

A contribuição realizada pelo Instituto Vero<sup>4</sup> na consulta pública promovida pelo CGI.br ressalta a necessidade de atenção especial às plataformas digitais durante períodos eleitorais. De acordo com a instituição, esses períodos demandam mecanismos mais rigorosos de transparência devido à influência significativa das redes sociais na formação de opinião pública e na implementação de projetos políticos.

O impacto das plataformas digitais nos processos eleitorais tem sido uma preocupação crescente, especialmente diante do aumento da desinformação on-line e de seu uso para fins de propaganda eleitoral (Muñoz, 2020). No Brasil, o Tribunal Superior Eleitoral (TSE)<sup>5</sup> estabeleceu colaborações com as principais plataformas digitais para construir soluções para mitigar esses efeitos e garantir eleições justas e transparentes.

A Justiça Eleitoral é responsável por possibilitar a expressão da vontade dos

3. Instituto Alana. Sobre o Instituto Alana. Disponível em: <https://alana.org.br>. Acesso em: 01 nov. 2024.

4. Instituto Vero. Sobre o Instituto Vero. Disponível em: <https://institutovero.org.br>. Acesso em: 01 nov. 2024.

5. BRASIL. Tribunal Superior Eleitoral. Sobre o TSE. Disponível em: <https://www.tse.jus.br>. Acesso em: 12 nov. 2024

eleitores, operacionalizando todos os procedimentos eleitorais para que se desenvolvam em harmonia e transparência, sem que estorvos possam desviar a soberania popular (Velloso; Agra, 2016). Dessa forma, é de extrema importância que sejam explorados os meios de manipulação de dados existentes nas plataformas digitais atuais para que se possa refletir sobre a responsabilidade da Justiça Eleitoral no uso de redes sociais para propaganda política. Portanto, o respeito rigoroso da LGPD e, especialmente da Resolução 23. 732/2024 do TSE e das que a substituam ou aprimorem, nas campanhas eleitorais, é essencial para garantir a integridade do processo democrático e a confiança do eleitorado. O cumprimento das normas de proteção de dados não apenas assegura a conformidade legal, mas também preserva os direitos dos eleitores, na condição de titulares dos dados pessoais, evitando manipulações indevidas e promovendo um ambiente eleitoral justo e transparente.

Assim, o início do uso das redes sociais nas campanhas eleitorais no Brasil trouxe tanto avanços quanto desafios. Por um lado, essas plataformas democratizaram o acesso à informação política e facilitaram o contato direto entre candidatos e eleitores. Por outro, evidenciaram a necessidade urgente de regulamentações mais completas e de uma educação digital abrangente para que o eleitor seja capaz de filtrar e compreender as informações de forma crítica. Contudo, essa democratização também requer que o sistema eleitoral esteja preparado para enfrentar os desafios da transparência e da veracidade das informações compartilhadas, a fim de evitar o abuso das plataformas digitais para a manipulação do eleitorado.

### **Transparência de dados e proteção de direitos de crianças e adolescentes nas plataformas digitais**

A defesa dos direitos de crianças e adolescentes nas plataformas digitais é um tema de relevância, especialmente diante do aumento da exposição desse público a conteúdos inadequados e práticas que podem comprometer sua integridade e desenvolvimento. O Instituto Alana, em sua contribuição à consulta pública promovida pelo CGI, enfatiza a necessidade de mecanismos mais rigorosos de transparência para monitorar e mitigar violações aos direitos desse grupo, em conformidade com o artigo 227 da Constituição Federal, que estabelece a prioridade absoluta na proteção de crianças e adolescentes.

A Lei Geral de Proteção de Dados (BRASIL, 2018), estabelece diretrizes específicas para a coleta, armazenamento e processamento de dados pessoais de crianças e adolescentes, reconhecendo sua condição de vulnerabilidade e a necessidade de proteção adicional. Essa legislação é complementada por esforços da Autoridade Nacional de Proteção de Dados (ANPD)<sup>6</sup>, que define normas voltadas para a segurança e privacidade das informações desse público, especialmente em plataformas digitais.

Entretanto, a prática revela desafios quanto a coleta de dados pessoais de crianças e adolescentes. Muitas plataformas digitais coletam dados de crianças e adolescentes sem transparência adequada ou consentimento explícito, contrariando os princípios da LGPD. Isso demanda um esforço conjunto entre governo, empresas e sociedade civil para assegurar que os dispositivos legais sejam cumpridos. Além disso, as empresas devem adotar medidas claras e éticas para informar usuários e responsá-

6. BRASIL. Autoridade Nacional de Proteção de Dados. Sobre a ANPD. Disponível em: <https://www.gov.br/anpd>. Acesso em: 20 nov. 2024.

veis sobre como os dados serão utilizados, reforçando a confiança no ambiente digital (Silva, 2023).

O consentimento parental, exigido pela LGPD, é um elemento central para garantir a transparência no uso de dados de menores. Como apontam Soares e Santos (2021), esse consentimento deve ser fornecido de forma clara e compreensível, permitindo que os responsáveis entendam os propósitos e implicações do uso das informações. Essa exigência reflete um alinhamento com o Estatuto da Criança e do Adolescente (ECA)<sup>7</sup>, que adota o princípio da proteção integral e busca mitigar riscos digitais.

Os desafios relacionados ao tratamento de dados no ambiente digital são amplificados pelo crescente uso de plataformas digitais por crianças e adolescentes. Segundo Silva e Souza (2021), o compartilhamento constante de informações nesses meios pode impactar negativamente o desenvolvimento psicológico e emocional dos menores, ao mesmo tempo em que expõe suas preferências e comportamentos a manipulações indevidas. A LGPD procura mitigar esses riscos ao exigir práticas responsáveis e éticas das empresas, incluindo auditorias regulares e medidas de proteção robustas.

A pesquisa TIC Kids Online Brasil<sup>8</sup> de 2021, conduzida pelo CGI e pelo CETIC.br, reforça a importância desse debate ao revelar que 93% das crianças e adolescentes entre 9 e 17 anos no Brasil têm acesso à Internet, sendo que 88% possuem perfis em redes sociais. Entre as atividades mais comuns, destacam-se o envio de mensagens instantâneas (78%), pesquisas escolares (71%) e o uso de aplicativos como WhatsApp, Instagram, TikTok e YouTube. Esse panorama evidencia a necessidade urgente de implementar mecanismos de

transparência mais rigorosos para proteger esse público, como propôs o Instituto Alana.

### **Proposta para critérios de transparência para dados pessoais e moderação**

A transparência é um elemento essencial para a governança ética e responsável das plataformas digitais, especialmente no que diz respeito ao uso de dados pessoais e à moderação de conteúdo. Para promover maior clareza e confiança, é necessário implementar medidas que contemplem tanto o uso de dados quanto os critérios de moderação. No que se refere aos dados pessoais, as plataformas devem fornecer informações claras e detalhadas sobre quais dados são coletados, como são utilizados e com quais finalidades. É fundamental que os usuários tenham acesso pleno aos seus dados, incluindo explicações sobre os motivos de sua coleta e seu uso em decisões algorítmicas. Além disso, as plataformas devem especificar as entidades com as quais compartilham esses dados, garantindo que medidas de proteção avançadas, como criptografia de ponta a ponta, controles rigorosos de acesso, detecção e resposta a incidentes em tempo real, bem como atualizações regulares dos sistemas de segurança, sejam aplicadas para proteger informações sensíveis e que auditorias independentes e regulares sejam conduzidas, com relatórios acessíveis ao público.

No contexto da moderação de conteúdos, é imprescindível que as plataformas publiquem de forma clara os critérios utilizados para moderar e curar conteúdos, incluindo a aplicação de sistemas automatizados e revisões realizadas por especialistas treinados, responsáveis por analisar e tomar decisões sobre conteúdos que podem violar as políticas da plataforma, garantindo um olhar crítico e contextual sobre o material publicado.

7. BRASIL. Lei nº 8.069, de 13 de julho de 1990. Estatuto da Criança e do Adolescente. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/18069.htm](https://www.planalto.gov.br/ccivil_03/leis/18069.htm). Acesso em: 20 nov. 2024.

8. COMITÊ GESTOR DA INTERNET NO BRASIL. Pesquisa TIC Kids Online Brasil. Disponível em: <https://www.cetic.br/pt/tics/kids-online/>. Acesso em: 18 nov. 2024.

Relatórios regulares devem apresentar métricas qualitativas e quantitativas, como o número de conteúdos removidos ou bloqueados e as justificativas para essas ações. Quando sistemas automatizados são usados, é essencial detalhar seu funcionamento, suas limitações e os impactos gerados na curadoria de conteúdo. As plataformas também devem implementar medidas específicas para proteger a liberdade de expressão, especialmente no caso de conteúdos de interesse público, como materiais jornalísticos e artísticos, e divulgar informações sobre solicitações governamentais de remoção ou restrição de conteúdo.

Outro ponto relevante é a criação de mecanismos de recurso acessíveis para os usuários contestarem decisões de moderação, acompanhados de relatórios sobre os resultados desses processos. A educação dos usuários também é essencial para ampliar a transparência. Guias e materiais educativos devem ser elaborados para explicar, de forma clara e didática, as políticas de privacidade e moderação. Por fim, é necessário que as plataformas disponibilizem relatórios periódicos sobre o cumprimento das diretrizes de transparência, incluindo avaliações conduzidas por auditorias independentes, e que promovam o engajamento de diversos atores, como governos, sociedade civil e especialistas, na formulação e na avaliação dessas políticas.

## Proposta de regulação para plataformas digitais

Essas medidas têm como objetivo não apenas melhorar a governança digital, mas também fortalecer a confiança e o empoderamento dos usuários frente às plataformas digitais.

As plataformas digitais devem cumprir obrigações para garantir a transparência e a responsabilidade em suas operações, promovendo um ambiente inclusivo, ético e respeito-

so aos direitos humanos. Em primeiro lugar, os termos de serviço devem estar disponíveis na íntegra nas línguas oficiais e principais de todos os países em que atuam, assegurando que os usuários possam interagir, reportar problemas e apresentar reclamações em sua própria língua. É essencial que os sistemas de tradução automática utilizados sejam rigorosamente controlados para evitar falhas técnicas que prejudiquem a acessibilidade linguística. Os relatórios, avisos e processos de recurso devem ser disponibilizados na língua preferencial do usuário, garantindo acesso igualitário e eficaz a informações, especialmente para crianças e pessoas com deficiência, com adaptações apropriadas à faixa etária e às necessidades específicas.

No que diz respeito à proteção de crianças, as plataformas devem oferecer condições de serviço em linguagem apropriada e acessível, considerando o ponto de vista de um grupo diversificado de crianças, inclusive aquelas com deficiência, para garantir níveis iguais de acesso à informação. Os direitos das pessoas com deficiência devem ser contemplados em todas as interações, assegurando que possam compreender e utilizar os mecanismos de denúncia e recurso, que devem ser eficazes e acessíveis também para grupos em situações de vulnerabilidade e marginalização. Além disso, as plataformas digitais devem compreender as condições culturais locais ao responder às reclamações, criando sistemas de denúncia e recurso culturalmente sensíveis, rápidos e fáceis de usar, especialmente para crianças.

As plataformas devem priorizar denúncias de conteúdos que representem ameaças aos usuários, como violência e assédio, respondendo de forma célere e proporcionando canais específicos para agravamento de denúncias. É igualmente importante evitar o uso indevido dos sistemas de denúncia, estabele-

cendo salvaguardas contra comportamentos coordenados não autênticos. As plataformas devem também implementar mecanismos de recurso eficazes e confiáveis, disponíveis tanto na própria plataforma quanto em instâncias externas, permitindo que usuários, ou mesmo terceiros afetados, expressem suas preocupações e obtenham reparação adequada. Esses mecanismos devem ser baseados nos princípios de legitimidade, acessibilidade, previsibilidade, equidade, transparência, compatibilidade com direitos humanos e aprendizado contínuo.

Sempre que um conteúdo for removido, restringido ou sujeito a limitações, os usuários devem ser notificados de forma clara e detalhada, incluindo as razões para a ação, o método utilizado (automatizado ou humano) e as regras que embasaram a decisão. Além disso, os usuários devem ter o direito de recorrer de tais decisões por meio de processos estruturados e justos. As plataformas devem, ainda, realizar avaliações regulares do impacto de suas políticas, sistemas de moderação e abordagens algorítmicas sobre os direitos humanos, com foco nos riscos enfrentados por mulheres, meninas, jornalistas, artistas e defensores dos direitos humanos e do meio ambiente. Tais avaliações devem resultar em ajustes de políticas para mitigar riscos sistêmicos.

Por fim, as plataformas devem garantir a proteção da privacidade dos usuários, utilizando tecnologias avançadas que permitam a análise de dados internos por pesquisadores externos de forma segura, auxiliando na identificação de problemas como a amplificação algorítmica de conteúdos prejudiciais. Além disso, é fundamental assegurar o tratamento igualitário de organizações de notícias independentes e proteger contra o uso abusivo das regras de moderação e comunicação, promovendo um ambiente digital mais justo, transparente e inclusivo para todos.

### **Proposta para a criação de autoridades reguladoras independentes**

A criação de autoridades regulatórias independentes é essencial para monitorar as plataformas digitais, assegurar o cumprimento das normas e aplicar sanções em caso de violações. Essas autoridades devem operar de forma autônoma e livre de pressões econômicas, políticas ou de outras naturezas, sendo seu mandato e poderes definidos por lei. A independência deve ser garantida tanto em relação ao governo quanto às próprias plataformas, para evitar conflitos de interesse e promover a imparcialidade. As autoridades regulatórias devem responder prioritariamente aos órgãos legislativos, que supervisionam o cumprimento de seus mandatos, enquanto as intervenções estatutárias dessas entidades devem estar sujeitas à revisão judicial para evitar abusos de poder, decisões injustas, preconceituosas ou desproporcionais.

Essas instituições devem contar com financiamento adequado e transparente, proveniente de fontes claras e não sujeitas à discricionariedade governamental, garantindo recursos suficientes para desempenhar suas funções com eficácia. Seus dirigentes e membros devem ser selecionados por meio de processos participativos, transparentes, não discriminatórios e baseados no mérito. Além disso, é preciso que relatem anualmente suas atividades a um órgão independente, preferencialmente ao legislativo, e sejam responsabilizados por suas ações. Para evitar o tráfico de influência, após o término de seus mandatos, esses profissionais não poderão prestar serviços remunerados ou trabalhar para entidades reguladas por um período razoável.

As autoridades regulatórias independentes devem realizar auditorias periódicas obrigatórias, conduzidas por entidades externas e imparciais, que avaliem a conformidade das plataformas digitais com seus códigos de con-

duta, políticas e normas de autorregulação. Essas auditorias não devem ser financiadas diretamente pelas plataformas ou entidades da indústria para garantir a integridade do processo, ainda que taxas possam ser impostas para custear tais atividades. Os resultados dessas auditorias, bem como seus termos, devem ser disponibilizados para comentário público, promovendo maior transparência e prestação de contas.

Além disso, as autoridades devem poder exigir que as plataformas apresentem relatórios periódicos detalhando a aplicação de suas condições de serviço e as medidas adotadas para salvaguardar a liberdade de expressão e o acesso à informação e conteúdos culturais diversificados. Caso as plataformas não cumpram suas políticas ou normas internacionais de direitos humanos, as autoridades devem adotar medidas corretivas, emitir recomendações públicas — vinculativas ou não — e estabelecer diretrizes transparentes e adequadas. Essas diretrizes devem estar alinhadas com as normas internacionais de direitos humanos e devem incluir sanções específicas para plataformas que falhem em respeitar suas responsabilidades.

Por fim, as autoridades regulatórias independentes devem ser responsáveis pela criação de processos de reclamação acessíveis, tanto para usuários quanto para terceiros afetados pelas ações das plataformas. Esses processos devem assegurar que as violações sejam investigadas e que haja mecanismos claros e confiáveis para a aplicação de sanções, promovendo, assim, a transparência, a responsabilidade e a proteção dos direitos humanos no ambiente digital.

### Considerações Finais

Os desafios relacionados à regulação das plataformas digitais são complexos e demandam uma abordagem multifacetada, que integre princípios de transparência, responsabilidade e proteção dos direitos humanos. A análise dos textos evidencia a necessidade urgente de regulamentações complementares para lidar com questões como moderação de conteúdo, concentração de mercado, privacidade de dados e impacto na liberdade de expressão.

Os atuais marcos legais, como a LGPD, oferecem avanços importantes, mas permanecem insuficientes para enfrentar a escala e o impacto das plataformas no ambiente digital. A proposta de criação de autoridades regulatórias independentes surge como uma solução viável para monitorar e sancionar práticas abusivas, assegurando que as plataformas digitais operem em conformidade com normas éticas e legais. Além disso, mecanismos como auditorias externas, relatórios transparentes e processos acessíveis de reclamação são indispensáveis para promover a confiança e o empoderamento dos usuários.

As perguntas e respostas analisadas do CGI.br destacam a relevância de um diálogo contínuo entre governos, sociedade civil, especialistas e as próprias plataformas, buscando soluções que respeitem a diversidade cultural e os direitos individuais. No entanto, é importante que as plataformas sejam responsabilizadas por suas práticas e que sejam implementados mecanismos para prevenir abusos de poder e fortalecer a concorrência no mercado digital. ■

## Referências

ACQUISTI, A.; GROSS, R.; STUTZMAN, F. Privacy and modern technology: a cross disciplinary perspective. Springer, 2016.

ARAÚJO, Willian Fernandes. Norma algorítmica como técnica de governo em plataformas digitais: um estudo da Escola de Criadores de Conteúdo do YouTube. *Revista Fronteiras: estudos midiáticos*, São Leopoldo, v. 23, n. 1, p. 29-39, jan./abr. 2021.

BARLOW, John Perry. Declaração de Independência do Cyberspaço. Davos, Suíça, 8 fev. 1996. Disponível em: <http://www.dhnet.org.br/ciber/textos/barlow.htm>. Acesso em: 23 dez. 2020.

BELLI, L.; FRANCISCO, P. A.; ZINGALES, N. Law of the land or law of the platform? Beware of the privatisation of regulation and police. In: BELLI, L. How platforms are regulated and how they regulate us. FGV, 2017.

BRASIL. Lei n.º 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. *Diário Oficial da União: seção 1*, Brasília, DF, p. 1, 24 abr. 2014.

BRASIL. Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/leis/L13709.htm](https://www.planalto.gov.br/ccivil_03/leis/L13709.htm). Acesso em: 14 nov. 2024.

BURGESS, Jean. Platform Studies. In: CUNNINGHAM, Stuart; CRAIG, David (ed.). *Creator culture: an introduction to global social media entertainment*. New York: NYU Press, 2021. p. 21-38.

BUSCH, C.; SCHULTE-NÖLKE, H.; WIEWIÓROWSKA-DOMAGALSKA, A.; ZOLL, F. The rise of the platform economy: a new challenge for EU Consumer Law? Christoph Busch et al., *The Rise of the Platform Economy: A New Challenge for EU Consumer Law*, 15 fev. 2016.

CHADWICK, Andrew. *The hybrid media system: politics and power*. 2. ed. New York: Oxford University Press, 2017.

COMITÊ GESTOR DA INTERNET NO BRASIL. Consulta sobre Regulação de Plataformas Digitais. [s.d.]. Disponível em: <https://dialogos.cgi.br/documentos/debate/consulta-plataformas/>. Acesso em: 18 nov. 2024.

COMITÊ GESTOR DA INTERNET NO BRASIL. Diálogos CGI.br: sobre o projeto. [s.d.]. Disponível em: <https://dialogos.cgi.br/sobre/>. Acesso em: 8 nov. 2024.

COMITÊ GESTOR DA INTERNET; CETIC.br. Pesquisa TIC Kids Online: Brasil 2022: crianças e adolescentes. [2022].

CORIAT, Benjamin. *El taller y el robot: ensaios sobre el fordismo e a produção em massa em la era de la electrónica*. Siglo XXI, 2011.

D'ANDRÉA, Carlos Frederico de Brito. *Pesquisando plataformas online: conceitos e métodos*. Salvador: EDUFBA, 2020.

EASTERBROOK, Frank H. *Cyberspace and the Law of the Horse*. University of Chicago Legal Forum, 1996. Disponível em: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi>. Acesso em: 14 dez. 2020.

FLORIDI, L. *The fourth revolution: How the infosphere is reshaping human reality*. Oxford: Oxford University Press, 2014.

GILLESPIE, T. The politics of 'platforms'. *New Media & Society*, v. 12, n. 3, p. 347-364, maio 2010.

LAKATOS, E. M.; MARCONI, M. de A. *Fundamentos de metodologia científica*. São Paulo: Atlas, 1992.

MUÑOZ, Óscar Sanchez. La regulación de las campañas electorales en la era digital. Valladolid: Univ. De Valladolid, 2020.

PASQUALE, F. Platform neutrality: enhancing freedom of expression in spheres of private power. *Theoretical Inquiries in Law*, v. 17, n. 2, p. 487-513, jul. 2016.

POELL, Thomas; NIEBORG, David; DUFFY, Brooke Erin. *Platforms and cultural production*. Cambridge, UK; Medford, MA: Polity Press, 2022.

SILVA, M. F. O impacto das recomendações da ANPD. *Revista de Tecnologia e Direito*, v. 11, n. 2, p. 88-100, 2023.

SOARES, E. A. G.; SANTOS, P. Ó.; DE JESUS, T. S. M. LGPD e a proteção de dados pessoais das crianças e adolescentes no ordenamento jurídico brasileiro: o dilema da coleta de dados e a obrigatoriedade do consentimento dos pais. *Revista Brasileira de Desenvolvimento*, [S. l.], v. 8, p. 76759-76774, 2021. DOI: 10.34117/bjdv7n8-072. Disponível em: <https://ojs.brazilianjournals.com.br/ojs/index.php/BRJD/article/view/33867>. Acesso em: 3 nov. 2024.

TRIVIÑOS, A. N. S. *Introdução à pesquisa em ciências sociais: a pesquisa qualitativa em educação*. São Paulo: Atlas, 1987.

YIN, R. K. *Estudo de caso: planejamento e métodos*. Porto Alegre: Bookman, 2001.

YIN, R. K. *Pesquisa qualitativa do início ao fim*. Porto Alegre: Penso, 2015.

ZUBOFF, Shoshana. *The age of surveillance capitalism*. New York: PublicAffairs, 2019.

### **Agradecimento**

*Esta pesquisa é financiada pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (Capes), por meio do Programa de Demanda Social.*

# Mídias sociais, regulação processual e dever de cuidado:

**evidências empíricas do debate no Brasil**

Palavras-chave [ regulação de plataformas; transparência de dados; período eleitoral; governança de dados; crianças e adolescentes ]



Ivar Hartmann, Ramon Costa, Bruno Oliveira

## Resumo

Este artigo investiga a regulação de plataformas digitais no Brasil, com foco na discussão do dever de cuidado nesse contexto. O objetivo é analisar como essa abordagem é apresentada e debatida na consulta pública sobre regulação de plataformas promovida pela CGL.br e na audiência pública do STF sobre a constitucionalidade do art. 19 do Marco Civil da Internet. A metodologia empregada é a análise documental qualitativa das contribuições nesses fóruns, buscando referências ao "dever de cuidado". Além disso, há uma revisão bibliográfica comparando a abordagem centrada no mérito do conteúdo com a abordagem centrada no mérito do procedimento. Os resultados demonstram o estado incipiente do debate sobre o dever de cuidado em plataformas e a importância de um processo regulatório para plataformas digitais que equilibre a liberdade de expressão com a prevenção de danos e a proteção do usuário.

## Introdução

É um fato bem conhecido que as plataformas que operam em mercados bilaterais (Parker et al., 2016) regulam o comportamento dos usuários em ambos os lados com um grau de poder e eficácia comparável à ação governamental (Belli e Zingales, 2017). No caso de plataformas de expressão, como as empresas de mídia social, o principal comportamento que regulam é a expressão. Essa ação regulatória das plataformas pode, à primeira vista, parecer semelhante à autorregulação tradicional, um modelo que existe há décadas (Ogus, 1995). No entanto, difere porque as empresas de mídia social não impõem limites à sua própria ação, mas sim às ações de seus usuários em ambos os lados do mercado (Hartmann, 2022).

A expressão online é um exemplo perfeito de comportamento humano regulado por quatro elementos distintos: normas sociais, a lei, o mercado e a arquitetura (Lessig, 1998). O principal incentivo das empresas de redes

sociais para censurar a expressão, contudo, é fomentar um ambiente agradável e familiar, propício ao aumento da receita publicitária (mercado) (Cohen, 2017; Klonick, 2017). Isso leva a casos de censura excessiva. Há muitos exemplos notórios: o Facebook, em determinado momento, removeu fotos de beijos gays (Hudson, 2011); plataformas costumavam remover fotos de amamentação (Locatelli, 2017); a foto da “Menina do Napalm”, uma obra de arte, também foi censurada (Ibrahim, 2017). A sociedade civil reagiu e garantiu revisões nas regras de moderação ou em sua aplicação. Isso demonstra que a moderação pode falhar em ambos os casos: por ser insuficiente ou excessiva. Atualmente, a tendência é de pressão da sociedade civil por uma moderação mais rigorosa.

Essa é a realidade no Brasil de 2024. Assolado por notícias falsas (Ribeiro e Ortellado, 2018) e discursos de ódio político (Silva, 2020; Ozawa et al., 2023) (MCI) (Lemos e Souza, 2016), o Congresso aprovou o projeto de lei multissetorial (Magalhães, 2015), rejeitando a prática de notificação e remoção de conteúdo devido aos seus efeitos inibidores perversos (Seltzer, 2010; Zingales, 2015). O Supremo Tribunal Federal (STF) também demonstrou disposição para reprimir as mídias sociais (Da Ros e Taylor, 2022) e começou a analisar se o art. 19 é uma solução constitucional para equilibrar a liberdade de expressão do usuário e os direitos das vítimas de conteúdo ilegal. Um processo judicial, em vez de um diálogo multissetorial que desencadeasse ação legislativa, coroou anos de desenvolvimentos no debate sobre moderação de conteúdo online no Brasil.

Em determinado momento nos últimos anos, o projeto de lei 2630/20, apelidado de “projeto de lei das notícias falsas”, mobilizou atenção e negociações como uma via para uma regulamentação sofisticada. Alguns

anos depois, em vez de um esforço para explorar os benefícios e desafios de múltiplas estratégias possíveis para a regulamentação de plataformas digitais, o país se depara com uma escolha superficial, exercida por um tribunal, entre notificação judicial e remoção de conteúdo e a notificação e remoção de conteúdo à moda antiga.

Existem duas desvantagens. Uma delas é o custo de retornar a um padrão de responsabilidade que induz à censura. Dados sobre remoção de conteúdo e valor de mercado antes e depois da MCI mostram que voltar ao sistema de notificação e remoção agora significaria uma perda anual de bem-estar do consumidor de até US\$ 740 milhões (Hartmann et al, 2023). A segunda desvantagem é menos óbvia e mais difícil de compreender. Trata-se do impacto negativo na qualidade do debate sobre a responsabilidade nas redes sociais e as soluções desejáveis.

O debate e a literatura sobre liberdade de expressão online no Brasil nunca foram particularmente ricos, frequentemente focando nas vantagens e desvantagens de diferentes padrões de responsabilidade. Por exemplo, a grande maioria dos projetos de lei propostos no Congresso entre 2014 e 2020 sobre responsabilização nas redes sociais adotou a resposta simplista de simplesmente substituir o art. 19 por um padrão de responsabilidade mais rigoroso (Hartmann e Lunes, 2020).

A abordagem do dever de cuidado foi raramente mencionada. O conceito está longe de ser estranho ao direito brasileiro. As obrigações do dever de cuidado derivam de interpretações de leis brasileiras, como o Estatuto da Criança e do Adolescente (ECA), o Código Civil, o Código do Consumidor e até mesmo de disposições constitucionais (Costa, 2008; Castro, 2017). O ordenamento jurídico brasileiro já estabelece um marco de deveres para a proteção de grupos vul-

neráveis, de modo que as plataformas também estão sujeitas ao cumprimento do dever de cuidado devido à natureza e à operação de seus negócios (Frazão, 2024). Especialmente após o fracasso do projeto de lei 2630/20, com a atenção voltada para o julgamento do STF, a regulamentação com base no mérito do conteúdo monopolizou o debate. Isso contrasta fortemente com a regulamentação com base no mérito do procedimento, como previsto pelos Princípios de Santa Clara<sup>1</sup>.

Os Princípios de Santa Clara são cruciais neste contexto, pois estabelecem diretrizes para auxiliar na regulamentação da moderação de conteúdo por plataformas digitais. Esses princípios foram desenvolvidos por um grupo de acadêmicos, especialistas e defensores dos direitos digitais em 2018, com o objetivo de proporcionar maior transparência e equidade nos processos de moderação de conteúdo. Assim, existe uma relação relevante entre os Princípios de Santa Clara e a discussão sobre a regulamentação e a responsabilização das plataformas digitais pelo conteúdo. Isso porque os princípios são guiados por aspectos como transparência, liberdade de expressão e proteção dos direitos do usuário.

Este artigo apresenta os fundamentos da regulação com base no mérito processual e, em seguida, descreve como a sociedade civil tem inserido essa estratégia regulatória no debate. Realizamos uma análise qualitativa das discussões em dois fóruns-chave: a consulta pública sobre plataformas digitais organizada pelo Comitê Diretivo da Internet e a consulta pública sobre o art. 19 e sua constitucionalidade, promovida pelo STF. Diante da diversidade da regulação com base no mérito processual, apresenta-

da na primeira seção deste artigo, optamos por focar no dever de cuidado para compreender como ele é apresentado, construído e argumentado nessas duas arenas cruciais para a participação da sociedade civil.

A pesquisa faz parte do projeto "Regulamentação de plataformas no Brasil e no Reino Unido: concepção e aplicação de marcos de 'dever de cuidado'", conduzido por meio de uma parceria entre a Universidade de Sussex, no Reino Unido, e o Insper, no Brasil, financiado pela Academia Britânica, com o apoio do Fundo de Parcerias Científicas Internacionais do governo britânico. Esta pesquisa teve como objetivo explorar a experiência do Reino Unido com a Lei de Segurança Online de 2023. O projeto produzirá evidências para subsidiar a abordagem brasileira à regulamentação de plataformas, especialmente considerando a falta de discussão sobre o princípio do dever de cuidado no desenvolvimento e implementação de um marco regulatório para plataformas digitais.

O artigo está estruturado da seguinte forma. Primeiramente, descrevemos a metodologia de pesquisa empregada para desvendar empiricamente o perfil do debate sobre o dever de cuidado como uma alternativa viável para a regulação de plataformas. Em seguida, apresentamos uma revisão da literatura sobre o contraste entre a regulação das mídias sociais com base nos méritos do conteúdo (em grande parte, padrões de responsabilidade) e com base nos méritos das garantias processuais, que refletem um dever de cuidado das plataformas em relação à liberdade de expressão dos usuários. Por fim, apresentamos e discutimos os resultados de nossa análise qualitativa.

---

1. Disponível em: <https://santaclaraprinciples.org>

## Metodologia

A metodologia deste artigo consiste em uma análise documental qualitativa das contribuições para a Consulta sobre a Regulação de Plataformas Digitais promovida pela CGI.br e para a audiência pública do STF sobre o Tema 987, que aborda a constitucionalidade do artigo 19 da Lei nº 12.965/2014 (Quadro Civil Brasileiro da Internet). Este artigo estabelece a necessidade de uma ordem judicial prévia e específica para a remoção de conteúdo, a fim de que provedores de serviços de Internet, websites e administradores de aplicativos de redes sociais sejam responsabilizados civilmente por danos decorrentes de atos ilícitos cometidos por terceiros.

Para atingir esse objetivo, utiliza-se a técnica de análise de comentários públicos em ambos os fóruns, com foco no tema do dever de cuidado. A audiência pública realizada pelo STF em 2023 para fundamentar sua decisão sobre o art. 19 contou com 47 participantes. Para identificar as declarações referentes ao dever de cuidado, buscamos o termo "cuidado" no documento contendo as transcrições da audiência (STF, 2023). Após identificar o uso dessa palavra, verificamos se ela foi mencionada em referência ao conceito de dever de cuidado. Em caso afirmativo, anotamos qual participante utilizou esse conceito e separamos sua apresentação para leitura e análise posteriores. Ao final desse processo, identificamos 12 participantes que se referiram ao "dever de cuidado".

A consulta pública sobre a regulamentação das plataformas digitais, organizada em 2023 pelo Comitê Diretivo da Internet do Brasil, recebeu 1.306 comentários. Utilizando um arquivo csv contendo todas as contribuições (CGI.br, s.d.), realizamos uma busca automatizada com código Python por comentários contendo as palavras "dever" e "cuida-

do", permitindo qualquer combinação de caracteres entre esses dois termos. Essa busca retornou doze comentários enviados por oito colaboradores diferentes. Uma busca similar pelos termos "dever" e "cuidado" em inglês não apresentou resultados.

Após identificar aqueles que mencionaram o dever de cuidado em cada um desses fóruns, procedemos à sumarização de suas contribuições. Em seguida, organizamos e sistematizamos as contribuições, que são apresentadas na seção de resultados.

Esta análise e categorização de discursos em dois importantes espaços de debate público sobre plataformas digitais visa destacar como um potencial regime de dever de cuidado está sendo concebido para um processo regulatório no Brasil. Cabe ressaltar que os fóruns possuem responsabilidades e procedimentos distintos, o que permite um escopo analítico mais amplo sobre como diferentes setores da sociedade civil estão se posicionando. As análises também possuem uma conexão especial com a revisão bibliográfica apresentada neste artigo, que detalha os procedimentos de moderação de conteúdo e a presença do dever de cuidado em um contexto regulatório para esses procedimentos, incluindo os direitos dos usuários e as responsabilidades das plataformas na mitigação e prevenção de riscos e danos causados por conteúdo de terceiros.

## Regulação processual das redes sociais

O âmbito da regulação pode ser o mérito do conteúdo ou o mérito dos procedimentos de moderação. Este último é norteador por uma preocupação com o devido processo legal (Citron, 2008). O primeiro é problemático, especialmente pela falta de precisão.

A qualidade da análise é insuficiente e os danos colaterais são consideráveis devido

às abordagens adotadas pela legislação da grande maioria dos países em relação a quem decide sobre o mérito de casos específicos de discurso. Os governos depositaram toda a sua confiança em decisões privadas automatizadas (Wu, 2019; OFCOM, 2019) ou em decisões tomadas por profissionais não oficiais (Barrett, 2020; Roberts, 2019), bem como em decisões públicas (judiciais) (Epstein, Parker e Segal, 2013; Keller, 2020) sujeitas a erros. O resultado até agora é que essas decisões pressionam ainda mais as plataformas contra a responsabilidade legal, enquanto a percepção da sociedade civil é de que a disseminação de desinformação (Wardle e Derakhshan, 2017) e discurso de ódio só aumentou.

## Dever de cuidado

O escopo da autorregulação da liberdade de expressão pode se restringir aos méritos do procedimento de moderação de conteúdo de uma plataforma. A supervisão regulatória pode se abster de focar nos méritos de uma publicação específica e, em vez disso, avaliar a qualidade dos processos implementados para sinalizar, detectar, revisar, tomar decisões e recorrer de decisões sobre o conteúdo do usuário. Enquanto muitos países continuam pressionando as empresas por resultados perfeitos de remoção de conteúdo, eles subestimam o custo para a liberdade de expressão decorrente da imprecisão inerente aos processos de moderação das plataformas.

Se o conteúdo ilegal for mantido em níveis suficientemente baixos, os legisladores não se sentirão inclinados a questionar o impacto na saúde dos moderadores humanos, o nível de precisão da inteligência artificial que toma ou auxilia nas decisões de moderação, ou a transparência de todo o sistema para os usuários. O devido processo legal na moderação de conteúdo deve ser reconhecido como

um fim em si mesmo, e não como um luxo. Abandonar a avaliação baseada no resultado do procedimento de moderação de uma plataforma em um caso específico resolve muitos problemas das alternativas tradicionais para analisar o mérito da expressão. Os tribunais não seriam sobrecarregados com processos sobre publicações individuais, e suas análises sobre o que a empresa deveria ter feito em um caso específico teriam pouca ou nenhuma importância. Os litígios teriam que questionar as falhas processuais gerais com base em evidências de múltiplos casos. A responsabilidade não dependeria unicamente do frágil julgamento de um tribunal sobre a legalidade de uma expressão isolada. Se uma empresa de mídia social cumpre as regras sobre o procedimento de moderação, ela não pode ser punida por causa de um único caso que passou despercebido e resultou em censura excessiva ou insuficiente.

As vantagens de abandonar as obrigações de resultado e focar no dever de cuidado, criando diretrizes processuais obrigatórias, são talvez mais visíveis no caso da moderação automatizada – algo que os governos têm incentivado recentemente as plataformas a aprimorar (Gorwa, Binns e Katzenbach, 2020). Atualmente, os governos analisam apenas uma pequena fração do que a caixa-preta do algoritmo de moderação produz (Tufekci, 2015). Não há uma forma de mensurar o desempenho do software com base em um conjunto de decisões representativo do todo. Uma decisão automatizada que não detectou discurso de ódio pode ser a exceção ou a regra, mas os formuladores de políticas, os usuários e terceiros afetados não têm a menor ideia. A responsabilidade pelo resultado em casos de moderação selecionados arbitrariamente não oferece incentivo para que as plataformas melhorem a precisão de seus aplicativos de inteligência artificial.

O desalinhamento fundamental de incentivos prejudica, portanto, os usuários, mas também as plataformas. A empresa não pode ser responsabilizada por decisões específicas emitidas por inteligência artificial desenvolvida propositalmente para operar de forma autônoma, decidindo sobre novas formas de expressão que os engenheiros poderiam ter previsto. A responsabilidade objetiva pelos resultados da moderação automatizada é equivocada e catastrófica para a inovação (Thierer, 2016). como responsabilidade objetiva para veículos autônomos<sup>2</sup>.

Em vez de impor um dever de resultado – zero conteúdo ilegal ou zero censura ilegal –, os governos podem definir diretrizes básicas para o procedimento de moderação e aplicar deveres de cuidado. Este é o modelo proposto pelo Livro Branco sobre Danos Online do governo do Reino Unido, baseado na constatação de que um dever de resultado aliado à responsabilização se mostrou uma solução ineficiente: “o foco na responsabilização pela presença de conteúdo ilegal não incentiva as melhorias sistêmicas nos processos de governança e gestão de riscos que consideramos necessárias”. O Livro Branco detalha um modelo com deveres de cuidado sob supervisão governamental.

Uma forma alternativa de responsabilização, no âmbito do dever de cuidado, poderia permitir que usuários e outras partes lesadas ainda responsabilizassem as empresas de mídia social, mas somente se os demandantes fossem além da discussão de uma única publicação e apresentassem alegações procedentes sobre as inadequações do procedimento como um todo. Essa distinção tem raízes no direito privado francês, que separa a obrigação de meio da obrigação de resultado. A obrigação de meio também é descrita como uma obrigação processual, segundo a qual uma empresa está vinculada a um plano

de vigilância que estabeleceu e pode ser acusada de não cumpri-lo (Cossart, 2017).

Neste contexto, a autorregulação regulamentada significa que as empresas de redes sociais têm alguma, mas não total, independência para definir os detalhes de seus procedimentos. Apresentaremos alguns elementos do devido processo legal para a moderação de conteúdo, mas já existem propostas na literatura, especialmente no que diz respeito à transparência. Os tribunais ou mesmo a Administração Federal de um determinado país não devem estabelecer esses elementos. É papel inescapável dos legisladores definir as diretrizes processuais gerais para a moderação. Um ponto de partida notavelmente avançado para legisladores em qualquer lugar do mundo é o conjunto de garantias processuais dos Princípios de Santa Clara.

Sem dúvida, uma abordagem baseada no dever de cuidado inclui responsabilizar os intermediários pelo conteúdo gerado por terceiros em suas plataformas. Ao passar de uma análise caso a caso para uma análise sistêmica, os governos poderiam aumentar a obrigação das plataformas de monitorar, identificar e remover ou mitigar conteúdo prejudicial, mesmo que gerado por terceiros. A implementação desse dever de cuidado varia de acordo com a jurisdição, mas, em geral, os intermediários devem tomar medidas razoáveis para evitar danos aos usuários (Machado; Aguiar, 2023).

Essa abordagem também deve considerar a necessidade de equilibrar a proteção dos direitos dos usuários com a preservação da liberdade de expressão. Há preocupação com o risco de censura caso as plataformas adotem uma abordagem excessivamente cautelosa na moderação de conteúdo, resultando na supressão indevida da liberdade de expressão. Portanto, o dever de cuidado deve ser equilibrado para preservar os direitos e

---

2. No mínimo, deveria haver um sistema diferenciado de responsabilidade que proteja as empresas que adotaram proativamente as melhores práticas recomendadas (Scherer, 2016).

mitigar danos e riscos, sem conceder carta branca para decisões de moderação de conteúdo que careçam de critérios objetivos e juridicamente sólidos.

## Garantias processuais como deveres de cuidado

### TRANSPARÊNCIA

A transparência das políticas substantivas e processuais da plataforma, bem como de sua aplicação efetiva, é fundamental. A legislação alemã já estabeleceu um conjunto claro de requisitos de acesso à informação (Wagner et al., 2020), que estão atualmente servindo de base para projetos de lei em outros países, como o Brasil.

A primeira dimensão da transparência é a informação sobre o todo. O primeiro dos três Princípios de Santa Clara, “números”, refere-se à transparência abrangente sobre a moderação efetivamente realizada, a fim de informar não apenas os usuários da rede social, mas também a sociedade civil em geral e as autoridades públicas. De acordo com esse princípio, a empresa é obrigada a fornecer relatórios periódicos em formato legível por máquina com o número total de decisões de moderação. Os relatórios devem detalhar as estatísticas descritivas de acordo com quatro variáveis: objeto da decisão (postagem ou usuário), tipo de decisão (denúncia ou remoção), origem da denúncia (decisão automatizada, governo, usuários etc.) e localização geográfica (do usuário que fez a denúncia e das partes afetadas).

O segundo princípio de Santa Clara também contém uma obrigação sobre moderação em abstrato: as regras substantivas e processuais adotadas pela plataforma devem ser acessíveis a todos. Nos dias de hoje, isso

pode parecer óbvio, mas não faz muito tempo, nem mesmo as maiores redes sociais forneciam suas políticas de conteúdo aos seus próprios usuários.

A segunda dimensão da transparência diz respeito à informação sobre a moderação no caso específico. O segundo princípio de Santa Clara trata da exigência de informações mais detalhadas para o usuário afetado, cuja expressão foi restringida. As plataformas devem informar o autor da publicação sobre o motivo específico da remoção, assim como um tribunal é obrigado a fornecer o fundamento jurídico de sua decisão. Elas também devem oferecer detalhes sobre o processo pelo qual a publicação foi identificada e considerada em conflito com a política de conteúdo. O usuário tem o direito de saber, por exemplo, se sua expressão foi restringida por um humano, por uma decisão automatizada ou por uma combinação de ambos. Além disso, a empresa também deve instruir o usuário sobre suas opções para questionar a decisão.

Os princípios de Santa Clara não contêm diretrizes específicas sobre a responsabilização ou explicabilidade da moderação algorítmica. A OCDE foi pioneira na elaboração de um conjunto de princípios sobre inteligência artificial que devem orientar os legisladores na definição das obrigações processuais das redes sociais em relação aos seus sistemas automatizados de moderação<sup>3</sup>. Ao longo dos anos, surgiram diversas listas de princípios e recomendações para o uso ético da inteligência artificial (Fjeld et al., 2020).

Princípios e recomendações éticas por si só, no entanto, não são suficientes. O uso da IA é generalizado em todo o mundo, em diferentes mercados, tanto por governos quanto por empresas privadas. Há ampla evidência de falhas que afetam desproporcionalmente

3. Os princípios de IA da OCDE mais úteis no contexto da moderação de conteúdo são: “Deve haver transparência e divulgação responsável em relação aos sistemas de IA para garantir que as pessoas compreendam os resultados baseados em IA e possam contestá-los” e “As organizações e os indivíduos que desenvolvem, implementam ou operam sistemas de IA devem ser responsabilizados pelo seu funcionamento adequado, em conformidade com os princípios acima”. Disponível em: <https://oecd.ai/en/ai-principles>.

as minorias. Os estudos em ciência da computação e engenharia oferecem conhecimento suficiente sobre o processo para permitir que os formuladores de políticas comecem a elaborar regras concretas, especialmente em setores onde o dano é irreparável (Black e Murray, 2019). Um requisito processual óbvio de transparência na moderação automatizada é a elaboração proativa de dados sobre a precisão. As plataformas devem começar configurando testes para verificar a precisão de seus modelos de aprendizado de máquina na identificação de diferentes tipos de conteúdo e anunciando periodicamente os índices de precisão (Davidson et al., 2017).

### **RECURSOS**

O terceiro princípio de Santa Clara estabeleceu a garantia fundamental do devido processo legal, ou seja, o direito de recorrer da remoção de conteúdo ou de uma punição aplicada à conta do usuário. A revisão da decisão de moderação de conteúdo deve ser feita por pessoas, após o usuário ter tido a oportunidade de apresentar sua defesa. Assim como na decisão original, a revisão precisa fornecer ao usuário a fundamentação política que a sustenta.

Assim como a transparência em geral, isso pode significar mais informações sobre as estratégias de moderação da plataforma para aqueles que persistentemente tentam burlá-las, como terroristas. No entanto, esse é um preço razoável a se pagar por uma redução da arbitrariedade da plataforma. Da mesma forma que a liberdade de expressão é crucial justamente para os discursos com os quais mais discordamos, o devido processo legal é fundamental, sobretudo, para aqueles que detestamos, como terroristas e supremacistas brancos. Uma garantia de apelação não está de forma alguma relacionada a uma avaliação dos méritos daquele caso específico

de discurso e não deve ser aplicável apenas a expressões online que a sociedade civil considera menos nocivas. Versões anteriores do projeto de lei 2630/20 incluíam essa diretriz processual como uma obrigação para as empresas de mídia social que operam no país.

### **OS TRIBUNAIS COMO EXECUTORES DAS GARANTIAS PROCESSUAIS DA LIBERDADE DE EXPRESSÃO**

Regras processuais para moderação de conteúdo podem ser o novo porto seguro para empresas de mídia social. Em vez de serem estritamente responsáveis, responsáveis após notificação ou após notificação judicial, as plataformas deveriam ser responsabilizadas apenas quando não cumprirem as diretrizes processuais consagradas em lei. Tais diretrizes exigirão regulamentação adicional por um órgão público independente com poder para consolidá-las, definindo regras e padrões para o procedimento, mas nunca para o mérito (Reino Unido, 2019). Essa autoridade poderia decidir, por exemplo, que discursos de ódio devem ser submetidos à revisão de cinco usuários e notícias falsas apenas a três. Mas jamais poderia, em hipótese alguma, arbitrar o mérito de uma publicação específica (Hartmann, 2020).

O novo papel dos tribunais seria o de apontar omissões importantes do legislador quanto às garantias processuais necessárias que devem ser concedidas aos usuários. Os tribunais também poderiam exercer uma supervisão limitada do trabalho da autoridade independente na definição de padrões para os procedimentos de moderação e, eventualmente, na aplicação de multas. No entanto, o Judiciário gradualmente deixaria de tomar decisões sobre o mérito de casos específicos de discurso. Uma possível transição seria a adoção inicial de um sistema de licenciamento, no qual a plataforma que cumpre todas as

normas sobre os procedimentos de moderação estaria sujeita a um padrão de responsabilidade diferente daquele da empresa que não cumpriu ou simplesmente optou por não aderir. Essa é uma solução atualmente em discussão para a regulamentação de aplicações de inteligência artificial, como veículos autônomos (Tutt, 2017).

É evidente que diferentes tipos de danos online exigem soluções específicas. Regular os procedimentos de moderação de conteúdo é mais eficaz do que apostar em padrões de responsabilidade para moderação de conteúdo baseados em uma análise centralizada do mérito da expressão. Um país pode preferir uma regulamentação mais rigorosa de notícias falsas do que de difamação, mas, em ambos os casos, o governo não deve impor às redes sociais uma obrigação de apresentar resultados. Os esforços de moderação de pornografia infantil e pornografia de vingança de uma empresa certamente devem estar sujeitos a requisitos mais rigorosos, mas também não podem ser considerados totalmente inadequados e passíveis de multas simplesmente porque uma entre milhares de publicações prejudiciais não é detectada e removida.

### **DEVER DE CUIDADO NA AUDIÊNCIA PÚBLICA DO STF**

Mais do que aqueles que mencionaram o conceito de dever de cuidado, chama a atenção aqueles que não o fizeram: representantes das principais redes sociais. Representantes do Facebook, Google, Twitter, Bytedance (TikTok Brasil) e Mercado Livre participaram da audiência pública, e nenhum deles discutiu o dever de cuidado. Por outro lado, o conceito foi mencionado por diversos órgãos governamentais<sup>4</sup>, organizações da sociedade civil<sup>5</sup> e

representantes de associações empresariais de outros setores ligados à Internet<sup>6</sup>. Esse fato parece indicar uma estratégia das empresas de mídia social para desviar a discussão sobre o Artigo 19 do Marco Civil da Internet no Supremo Tribunal Federal (STF) dos debates sobre a adoção do dever de cuidado ou do entendimento de que esse dever já possa existir de alguma forma no ordenamento jurídico brasileiro. Em contrapartida, diversos outros participantes buscaram defender a linha contrária, argumentando que as plataformas já deveriam aderir a um dever de cuidado.

Flávio Dino, então Ministro da Justiça e Segurança Pública (MJSP), argumentou que as plataformas violavam um dever de cuidado inerente a qualquer atividade econômica, conforme previsto no Código de Defesa do Consumidor. De forma semelhante, Estela Aranha, também falando em nome do MJSP, afirmou que o dever de cuidado era uma premissa fundamental das relações de consumo, enraizada no princípio da boa-fé. Isis Menezes Taboas, representante do Ministério da Mulher, também adotou a visão de que as plataformas já deveriam estar sujeitas a um dever de cuidado. No entanto, argumentou que esse dever decorria dos termos de uso das plataformas, que implicavam uma responsabilidade de supervisão e promoção de um ambiente seguro. As diferenças entre essas declarações, e o fato de outros representantes do governo não terem adotado uma posição semelhante quanto à existência de um dever de cuidado, indicam que não havia uma abordagem governamental coordenada sobre o que deveria ser defendido sobre esse tema.

Alguns representantes de organizações não governamentais também apoiaram interpretações que implicariam o reconhecimen-

4. Ministério da Justiça e Segurança Pública, Secretaria de Comunicação Social da Presidência da República, Escritório Nacional de Defesa da Democracia da Procuradoria-Geral da República – PNDD/AGU e Ministério da Mulher.

5. Comitê de Tecnologia e Inovação – OAB/SP, Instituto Brasileiro de Políticas e Direito do Consumidor, Instituto Alana, Instituto Brasileiro de Direito Civil – IBDCIVIL e Instituto de Tecnologia e Sociedade do Rio – ITS Rio.

6. Associação Brasileira de Internet (Abranet) e Associação Brasileira de Rádio e Televisão (Abratel).

to de um dever de cuidado já existente para as plataformas de mídias sociais no Brasil. Isabella Henriques, do Instituto Alana, defendeu uma interpretação sistemática e harmoniosa que reconheça que as normas do Marco Civil da Internet não podem se sobrepor a um dever geral de cuidado com o conteúdo consumido por crianças e adolescentes. Nessa perspectiva, mesmo em relação aos danos causados por conteúdo de terceiros, a interpretação de que a remoção de conteúdo ilícito depende de uma ordem judicial explícita deve ser rejeitada. Em vez disso, o dever de cuidado exigiria uma postura mais proativa, que vá além da mera remoção de conteúdo prejudicial assim que a plataforma tome conhecimento inequívoco dele. Uma vez que o dano está associado ao próprio modelo de negócios da plataforma, o dever de cuidado deveria se estender ao desenvolvimento da plataforma e de seus algoritmos.

Outros foram menos detalhistas, mas ainda reconheceram alguma forma de dever de cuidado já existente. João Quinelato, representando o Instituto Brasileiro de Direito Civil (IBDCIVIL), argumentou que a proteção da dignidade humana exige uma regulamentação que imponha responsabilidades proativas aos provedores, presumindo, portanto, deveres de cuidado. Da mesma forma, Aislan Vargas Basílio, da Associação Brasileira de Rádio e Televisão (Abratel), sugeriu similarmente um dever de cuidado baseado no princípio da boa-fé objetiva, como também proposto por Estela Aranha.

As demais declarações referentes ao dever de diligência podem ser divididas em dois grupos: as que defendem a adoção desse conceito e as que o criticam<sup>7</sup>. No primeiro grupo, João Brant, representando a Secretaria de Comunicação Social da Presidência da República, argumentou que a ausência de um

dever de diligência permite que as plataformas digitais permaneçam passivas. Essa escolha regulatória pode favorecer a liberdade de expressão, mas tornou-se evidente que essa abordagem é desequilibrada, visto que a proteção dos direitos autorais é mais forte na Internet do que a proteção contra ataques à democracia. Por essa razão, devem ser buscadas reformas no modelo atual, com cautela em relação aos potenciais efeitos inibidores que algumas alternativas regulatórias podem acarretar.

Marcelo Eugênio Feitosa Almeida, representando o Escritório Nacional de Defesa da Democracia da Procuradoria-Geral da República (PNDD/AGU), afirmou brevemente que a regulação das mídias sociais está passando de um modelo de ação estatal negativa para um modelo focado em ações positivas das plataformas, no qual o dever de diligência se situaria. Por fim, Carlos Affonso Souza, em nome da Associação Brasileira da Internet (Abranet), apresentou o dever de cuidado como uma das alternativas para aprimorar o Artigo 19 do Marco Civil da Internet brasileiro.

Entre os críticos do dever de cuidado, Ronaldo Lemos, falando em nome da Comissão de Tecnologia e Inovação da Ordem dos Advogados do Brasil, Seção São Paulo (OAB/SP), e Fabio Steibel, do Instituto de Tecnologia e Sociedade do Rio (ITS Rio), defenderam maior cautela na adoção de modelos estrangeiros, incluindo o dever de cuidado. Lemos argumentou que o aprimoramento do modelo brasileiro deve ser guiado por experiências bem-sucedidas do passado, como a regulação da pornografia de vingança, onde esse tipo de conteúdo foi definido como uma exceção que justifica o desvio da regra geral do artigo 19. Ele sugeriu a criação de outras exceções claramente definidas. Conceitos abertos como o dever de cuidado, segundo ele, seriam subjetivos e difíceis de aplicar,

---

7. A declaração de Guilherme Magalhães Martins, em nome do Instituto Brasileiro de Políticas e Direito do Consumidor, menciona o dever de cuidado, mas não aprofunda o tema. Portanto, não está agrupada com nenhum conjunto de declarações.

concedendo discricionariedade excessiva às plataformas e diminuindo o papel do judiciário ao transferi-lo para as corporações. Como modelo alternativo, Lemos propôs a autorregulação regulamentada, com órgãos de supervisão tendo autoridade vinculante para fiscalizar as atividades de moderação da rede e estabelecer regras de transparência, orientando as plataformas para uma melhor tomada de decisão. Steibel expressou preocupações semelhantes, destacando os riscos de conceder ainda mais poder às plataformas e levar à moderação excessiva.

### **DEVER DE CUIDADO NA CONSULTA PÚBLICA DO CGI.BR**

A análise do dever de cuidado no contexto brasileiro da regulação de plataformas envolve essencialmente o debate público, considerando a participação de atores multissetoriais na regulação de plataformas digitais no país. Nesse sentido, por meio do Grupo de Trabalho de Regulação de Plataformas, o CGI.br realizou a “Consulta sobre a Regulação de Plataformas Digitais”, com o objetivo de reunir diversas perspectivas sobre a regulação de plataformas. Essa consulta possui significativa relevância e impacto para a sociedade civil, visto que o Comitê tem desempenhado um papel importante em discussões sobre questões relacionadas à Internet, incluindo seu engajamento e participação em processos legislativos como o Marco Civil da Internet e a Lei Geral de Proteção de Dados (LGPD) (Cappi; Oms, 2023).

Todas as menções ao dever de cuidado vie-

ram de participantes associados a organizações especializadas em regulamentação da Internet<sup>8</sup> ou com experiência profissional na área<sup>9</sup>. Essas menções não se concentraram em nenhuma pergunta específica feita na consulta pública. Em vez disso, apareceram em respostas a nove perguntas diferentes, com não mais do que dois comentários mencionando o dever de cuidado em resposta à mesma pergunta.

Embora esta amostra seja pequena em comparação com o total (0,9%), limitando inferências e comparações mais amplas entre grupos de comentários que mencionam ou não este conceito, é importante notar que os comentários que mencionam o dever de cuidado são significativamente mais longos do que a média dos comentários submetidos na consulta. Os comentários que mencionam o dever de cuidado apresentaram uma média de 5.298 caracteres e uma mediana de 2.487 caracteres, enquanto aqueles que não o mencionam apresentaram médias de 1.310 e 590 caracteres, respectivamente<sup>10</sup>. Se a extensão dos comentários puder ser usada como uma métrica para estimar sua complexidade ou completude, esses dados quantitativos indicam uma correlação entre comentários que mencionam o dever de cuidado e comentários mais abrangentes e complexos – possivelmente explicada pelo perfil dos participantes que abordaram esse conceito, como mencionado anteriormente.

Outra descoberta quantitativa que corrobora essa observação é que, com exceção dos dois comentários mais curtos que mencionam o dever de cuidado, os outros dez

8. Alana Institute, Digital Rights Coalition, Electronic Frontier Foundation e Access Now, ABERT - Associação Brasileira de Emissores de Rádio e Televisão, ITS Rio e CTS-FGV.

9. Flávio Rech Wagner é professor do Instituto de Informática da UFRGS. Foi presidente do Capítulo Brasileiro da Internet Society, fundou e presidiu a Sociedade Brasileira de Computação e foi membro do Comitê Diretivo da Internet – CGI.br e NIC.br. Flávia Lefèvre Guimarães foi coordenadora do departamento jurídico do Idec, membro do Conselho Consultivo da Anatel e conselheira do Comitê Diretivo da Internet. Atualmente, trabalha como advogada.

10. Essa diferença persiste mesmo se excluirmos da comparação os comentários da consulta pública que respondem a outros comentários e, portanto, podem ser, em média, mais curtos, já que tendem a apenas concordar ou complementar brevemente os comentários anteriores. Sem esse subconjunto de comentários, o comprimento médio dos comentários aumentou ligeiramente para 1.358 caracteres e a mediana para 625 caracteres.

estão muito próximos<sup>11</sup> ou dentro do quartil dos comentários mais longos. Além disso, quatro comentários (um terço dos que mencionam o dever de cuidado) estão entre os 5% de comentários mais longos, incluindo o segundo mais longo no geral.

Em relação ao conteúdo dos comentários, quatro participantes manifestaram apoio à incorporação do dever de cuidado no ordenamento jurídico brasileiro, dois se opuseram e, em dois casos, não ficou claro se os participantes eram a favor ou contra esse modelo de responsabilidade. Por exemplo, Flávio Rech Wagner (id nº 715)<sup>12</sup> manifestou-se apenas contra a atuação da CGI.br na avaliação de relatórios de conformidade com o dever de cuidado elaborados por plataformas digitais, argumentando que a CGI.br não deveria assumir responsabilidades típicas de órgãos estatais. Essa posição não endossa nem rejeita o dever de cuidado, mas apenas afirma que a CGI.br não deveria ter tal função.

A outra posição ambígua veio de Carlos Affonso Souza, em nome do ITS Rio. Por um lado, o ITS Rio (id nº 1119) argumentou que a adoção de mecanismos de notificação e ação sem responsabilidade direta por conteúdo específico de terceiros poderia levar a ineficiências, potenciais violações da liberdade de expressão e suscetibilidade a abusos por parte dos usuários. Por outro lado, em um comentário separado (id nº 1124) que pressupunha a adoção do dever de cuidado sem criticá-lo explicitamente, o ITS Rio defendeu que as sanções administrativas por descumprimento do dever de cuidado deveriam se concentrar no conteúdo como um sistema para evitar o cerceamento do debate público. Segundo essa visão, seria possível alinhar o atual marco do

Marco Civil da Internet com disposições para sanções administrativas por descumprimento dos deveres de risco sistêmico.

Entre os comentários favoráveis à adoção do dever de cuidado, o Centro de Tecnologia e Sociedade da FGV Rio fez a observação mais sucinta, mencionando-o apenas como uma medida de mitigação sugerida para operações de influência em plataformas (id nº 1069). Flávia Lefèvre Guimarães enfatizou que o dever de cuidado não seria tão inovador quanto possa parecer, argumentando que se alinha ao princípio da responsabilidade previsto no Artigo 3º do Marco Civil da Internet e às disposições existentes no Código de Defesa do Consumidor, na Lei Geral de Proteção de Dados, no Código Eleitoral, no Código Civil e no Estatuto da Criança e do Adolescente (id nº 859). Ela defendeu a regulamentação desse dever por meio do Projeto de Lei 2630, destacando sua inspiração na Lei de Serviços Digitais, e sugerindo que o Código de Defesa do Consumidor e o Marco Civil da Internet já poderiam servir de base para uma maior responsabilização.

João Coelho, representando o Instituto Alana, e Rodolfo Salama, em nome da ABERT – Associação Brasileira de Emissoras de Rádio e Televisão – compartilharam opiniões semelhantes às de Flávia Lefèvre Guimarães. A ABERT também apoiou o modelo proposto pelo Projeto de Lei 2630 (id nº 920), elogiando particularmente o Artigo 11 do projeto, que lista os crimes a serem prevenidos e mitigados no âmbito do regime de dever de cuidado. Sugeriu ainda a inclusão de crimes eleitorais nessa lista. O Instituto Alana argumentou que a legislação vigente já impõe um dever de cuidado às plataformas (id nº

11. Como existem 1.306 comentários, o primeiro quartil vai até a posição 326. O décimo comentário mais longo que menciona o dever de cuidado está na posição 327.

12. Indica o número do comentário no documento da consulta de plataformas do CGI.br que baseou a pesquisa apresentada neste texto: <https://dialogos.cgi.br/documentos/debate/consulta-plataformas/> O documento também está em anexo na publicação no site da poliTICS.

805), especialmente no que diz respeito aos direitos de crianças e adolescentes. O instituto incluiu um parecer jurídico da Professora e Advogada Ana Frazão, também citado em outro comentário (id nº 806), que sugeriu a extensão do dever de cuidado quando as plataformas amplificam ou monetizam conteúdo gerado pelo usuário.

Em oposição ao dever de cuidado, Bia Barbosa, representando a Digital Rights Coalition, e Veridiana Alimonti, em nome da Electronic Frontier Foundation e da Access Now, apresentaram dois comentários cada. A Digital Rights Coalition expressou preocupação com o potencial de vigilância decorrente da imposição de um dever de cuidado, particularmente se este se estender a serviços de mensagens privadas (id nº 1267). Em outro comentário (id nº 1328), a coalizão argumentou explicitamente contra a atribuição de um dever de cuidado às plataformas, defendendo que estas não devem julgar o que constitui conteúdo criminoso nem decidir o que deve circular. Contudo, no mesmo comentário, a coalizão propôs um meio-termo: um regime em que as plataformas teriam obrigações de avaliação de risco e ação apenas em casos específicos, como ameaças graves e iminentes à integridade física, à saúde pública ou à democracia, incluindo pandemias, ataques terroristas ou outros perigos sérios.

De forma semelhante, a Electronic Frontier Foundation e a Access Now defenderam o abandono das obrigações de diligência para mitigar os riscos de abuso em regulamentações baseadas em conteúdo, privilegiando as avaliações de impacto sistêmico (id nº 1125). Em relação à diligência proposta no Projeto de Lei 2630/2020, as organizações criticaram o amplo escopo de atividades ilegais a serem controladas pelas plataformas, abrangendo seis leis

e 40 diferentes crimes, muitos dos quais com exceções (id nº 1129). Essa abrangência dificultaria a aplicação da lei, agravada pela falta de clareza sobre como e quais instituições avaliariam a conformidade. Essa regulamentação colocaria as plataformas em um papel judicial, o que elas consideraram inadequado.

## Considerações Finais

O caminho a seguir após a decisão do STF sobre o art. 19 e a responsabilidade dos intermediários é incerto. Dependerá de como a responsabilização nas redes sociais se consolidará à medida que os tribunais inferiores aplicarem a decisão do STF e as plataformas adaptarem seus termos e condições, bem como seus sistemas de moderação de conteúdo. Uma coisa permanece certa: simplificar o debate sobre alternativas de responsabilização não beneficia nenhuma das partes envolvidas.

O dever de cuidado e outras abordagens de regulação processual podem coexistir com diferentes padrões de responsabilidade, se necessário. As obrigações legais das plataformas quanto à qualidade dos procedimentos de moderação podem complementar eficazmente até mesmo padrões de responsabilidade mais rigorosos, como a notificação e remoção de conteúdo. A experiência do Reino Unido pode oferecer lições úteis para o Brasil, além de exemplos de advertência. Para distinguir as aplicações improdutivas ou ineficientes do dever de cuidado daquelas que poderiam promover a proteção dos direitos dos usuários no Brasil, é necessário um debate mais aprofundado sobre as características e os desafios dessa abordagem.

Demonstramos que, em dois fóruns cruciais para a participação da sociedade civil na regulamentação das redes sociais, a proporção do debate dedicada ao dever de cuidado

foi muito pequena. As raras contribuições, contudo, desempenharam um papel importante ao fornecer mais contexto e nuances às discussões sobre como coibir conteúdo abusivo online, garantindo, ao mesmo tempo, que as plataformas digitais não descartem o essencial junto com o supérfluo.

Nos próximos anos, à medida que a sociedade brasileira honra sua tradição de genuína partici-

pação multissetorial na governança da Internet, não deve permitir que uma única decisão judicial monopolize os esforços para encontrar opções viáveis de regulação das redes sociais. Seja por meio do projeto de lei 2630/20 em versão reformulada ou de uma proposta totalmente nova, a sociedade civil deve instar o Congresso a construir uma substituição democraticamente responsável para o art. 19 da MCI. ■

***Ivar hartmann** é professor associado de direito do Insper. É membro fundador da Platform Governance Research Network e afiliado ao International Panel on the Information Environment. Sua pesquisa foca a moderação de conteúdo online e tecnologia aplicada à pesquisa quantitativa em direito.*

***Ramon Costa** é professor de direito do insper. Doutor em direito pela PUC-Rio. Pesquisador do Núcleo Legalite: direito e novas tecnologias, da PUC-Rio.*

***Bruno Oliveira** é bacharel em direito pela Universidade de São Paulo. Mestre em direito e desenvolvimento pela Escola de Direito de São Paulo da Fundação Getúlio Vargas. Pesquisador do núcleo de saúde do Centro de Gestão e Políticas Públicas do Insper.*

## Referências

BARRETT, Paul M. Quem modera os gigantes das mídias sociais? Um apelo para acabar com a terceirização. Relatório NYU Stern , 2020. Disponível em: <https://www.stern.nyu.edu/experience-stern/faculty-research/who-moderates-social-media-giants-call-end-outsourcing> .

BELLI, Luca; ZINGALES, Nicolo (orgs.). Regulamentação de plataformas: como as plataformas são reguladas e como elas nos regulam . Resultado oficial da Coalizão Dinâmica do Fórum de Governança Intergovernamental da ONU sobre Responsabilidade de Plataformas. FGV Direito Rio, 2017. Disponível em: <https://hdl.handle.net/10438/19402>.

BLACK, Julia; MURRAY, Andrew. Regulamentação da IA e do aprendizado de máquina: definindo a agenda regulatória. *European Journal of Law and Technology* , v. 10, n. 3, 2019.

CASTRO, Thamis de. A Função da Cláusula de Bons Costumes no Direito Civil e a Teoria Tríplice da Autonomia Privada Existencial. *Revista Brasileira de Direito Civil* , v. 14, 2017, p. 99-125.

CITRON, Danielle Keats. Devido Processo Tecnológico. *Washington University Law Review* , v. 85, 2008.

COHEN, Julie E. Direito para a Economia de Plataformas. *UCD Law Review* , v. 51, 2017, p. 165.

COSSART, Sandra; et al. A Lei Francesa sobre o Dever de Cuidado: Um Passo Histórico para Fazer a Globalização Funcionar para Todos. *Business and Human Rights Journal* , v. 2, p. 321, 2017.

COSTA, Judith H. Martins. Um Aspecto Da Obrigação De Indenizar: Notas Para Uma Sistematização Dos Deveres Pré-negociais De Proteção No Direito Civil Brasileiro. *Revista dos Tribunais* , v. 867, 2008, p. 11-51.

CAPPI, Juliano; OMS, Juliana. Sistematização das contribuições à consulta sobre regulação de plataformas digitais. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2023.

DA ROS, Luciano; TAYLOR, Matthew M. Bolsonaro e o Judiciário: entre acomodação e confronto. In: BIRLE, Peter; SPECK, Bruno (eds.). *Brasil sob Bolsonaro. Quão ameaçada está a democracia?* . Instituto Ibero-Amerikanisches Preußischer Kulturbesitz, 2022. p. 1-20.

DAVIDSON, Thomas; et al. Detecção automatizada de discurso de ódio e o problema da linguagem ofensiva. In: *Anais da 11ª Conferência Internacional da AAI sobre Web e Mídias Sociais* , 2017, p. 1.

DAVIDSON, Thomas; et al. Detecção automatizada de discurso de ódio e o problema da linguagem ofensiva. In: *Anais da 11ª Conferência Internacional da AAI sobre Web e Mídias Sociais* , 2017.

DIÁLOGOS CGI.BR. Consulta sobre Regulação de Plataformas Digitais. Disponível em: <https://dialogos.cgi.br/documentos/debate/consulta-plataformas/>.

EPSTEIN, Lee; PARKER, Christopher M.; SEGAL, Jeffrey A. Os juízes defendem o discurso que odeiam? Viés intragrupal, oportunismo e a Primeira Emenda. In: Encontro Anual da Associação Americana de Ciência Política, 2013.

' O Dilema das Redes' erra. 2020. Disponível em: <https://about.fb.com/wp-content/uploads/2020/10/What-The-Social-Dilemma-Gets-Wrong.pdf>

FJELD, Jessica; et al. Inteligência Artificial com Princípios: Mapeando o Consenso em Abordagens Éticas e Baseadas em Direitos para Princípios de IA. Berkman Klein Center, Publicação de Pesquisa nº 2020-1, 2020.

FRAZÃO, Ana. A responsabilidade civil das plataformas digitais por conteúdos de terceiros diante do artigo 19 do Marco Civil da Internet. In: FRAZÃO, Ana; MULHOLAND, Caitlin; POLIDO, Fabrício Bertini Pasquot (Coords.). Marco Civil da Internet: impactos, evoluções e perspectivas. São Paulo: Thomson Reuters Brasil, 2024. p. 17-41.

GORWA, Robert; BINNS, Reuben; KATZENBACH, Christian. Moderação algorítmica de conteúdo: desafios técnicos e políticos na automação da governança de plataformas. *Big Data & Society*, 2020, p. 1-15.

HARTMANN, I.; et al. Análise econômica da responsabilidade das redes sociais. *Economic Analysis of Law Review*, v. 14, n. 2, 2023, pp. 17-41.

HARTMANN, I.; IUNES, J. Fake News No Contexto De Pandemia E Emergência Social: Os Deveres E Responsabilidades Das Plataformas De Redes Sociais Na Moderação De Conteúdo Online Entre A Teoria E As Proposições Legislativas. *Revista Direito Público*, v. 94, 2020, pp.

HARTMANN, Ivar A. Uma nova estrutura para moderação de conteúdo online. *Computer Law & Security Review*, v. 36, 2020.

HARTMANN, Ivar A. Autorregulação em plataformas de conteúdo online e a proteção dos direitos da personalidade. In: ALBERS, Marion; SARLET, Ingo (orgs.). Proteção dos Direitos da Personalidade e Proteção de Dados Online. Springer, 2022.

HUDSON, John. A controvérsia sobre a proibição de beijos gays no Facebook não acabou. *The Atlantic*, 2011. Disponível em: <https://www.theatlantic.com/technology/archive/2011/04/controversy-over-facebooks-gay-kissing-ban-isnt-over/349921/>.

IBRAHIM, Yasmin. Facebook e a Garota do Napalm: Reenquadrando o Icônico como Pornográfico. *Social Media + Society*, out-dez 2017, p. 1.

KELLER, Clara Iglesias. Política por judicialização: o marco institucional da responsabilidade dos intermediários no Brasil. *Revista Internacional de Direito, Computadores e Tecnologia*, 2020.

KLONICK, Kate. Os Novos Governadores: As Pessoas, as Regras e os Processos que Regem a Liberdade de Expressão Online. *Harvard Law Review*, v. 131, 2018.

LEMONS, Ronaldo; SOUZA, Carlos Affonso. Marco Civil da Internet – Construção e Aplicação. Juiz de Fora: Editar, 2016.

LESSIG, Lawrence. A nova escola de Chicago. *The Journal of Legal Studies*, v. 27, n. 2, 1998.

LOCATELLI, Elisabetta. Imagens de amamentação no Instagram: autorrepresentação, publicidade e gestão da privacidade. *Social Media + Society*, abril de 2017.

MACHADO, Caio CV; AGUIAR, Thaís Helena. Regulamentações emergentes sobre moderação de conteúdo e políticas de desinformação em plataformas de mídia online: incorporando o dever de cuidado em modelos de responsabilidade intermediária. *Business and Human Rights Journal*, v. 8, p. 244-251, 2023.

MAGALHÃES, João Carlos. Imaginando criticamente a governança da Internet: uma análise de conteúdo da Consulta Pública do Marco Civil da Internet. Série de dissertações de mestrado MEDIA@LSE, 2015.

OFCOM. Uso de IA na moderação de conteúdo online. Cambridge Consultants/OFCOM,

2019. Disponível em: <https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/other/cambridge-consultants-ai-content-moderation.pdf?v=324081>.

OFCOM. Uso de IA na moderação de conteúdo online. Relatório, 2019. Disponível em: [https://www.ofcom.org.uk/\\_\\_data/assets/pdf\\_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf](https://www.ofcom.org.uk/__data/assets/pdf_file/0028/157249/cambridge-consultants-ai-content-moderation.pdf).

OGUS, Anthony. Repensando a autorregulação. *Oxford Journal of Legal Studies*, v. 15, 1995.

OZAWA, João VS; et al. Como a desinformação no WhatsApp passou de arma de campanha a propaganda governamental no Brasil. *Social Media + Society*, v. 9, n. 1, 2023, p. 1-12.

PARKER, Geoffrey; VAN ALSTYNE, Marshall W.; CHOUDARY, Sangeet Paul. *Revolução das Plataformas: Como os Mercados em Rede Estão Transformando a Economia e Como Fazê-los Funcionar para Você*. WW Norton & Company, 2016.

RIBEIRO, Márcio Moretto; ORTELLADO, Pablo. Notícias falsas: o que são e como lidar com elas. *Sur*, v. 15, n. 27, 2018, p. 1-12.

ROBERTS, Sarah T. *Por trás da tela: Moderação de conteúdo nas sombras das mídias sociais*. Yale University Press, 2019.

SCHERER, Matthew U. Regulamentação de Sistemas de Inteligência Artificial: Riscos, Desafios, Competências e Estratégias. *Harvard Journal of Law and Technology*, v. 29, p. 357, 2016.

SELTZER, Wendy. Liberdade de expressão desvinculada da proteção do direito autoral: efeitos inibidores da DMCA sobre a Primeira Emenda. *Harvard Journal of Law and Technology*, v. 24, 2010.

SILVA, Daniel N. A Pragmática do Caos: Analisando a Linguagem Antidemocrática de Bolsonaro. *Trabalhos em Linguística Aplicada*, v. 1, 2020, pág. 507-537.

SUPREMO TRIBUNAL FEDERAL - STF. RE 1.037.396 e RE 1.057.258 – Responsabilidade civil dos provedores por conteúdo ilícito gerado por terceiros. Transcrições da 38ª audiência pública. Ministros-Relatores Dias Toffoli e Luiz Fux. Brasília: Supremo Tribunal Federal/Secretaria Judiciária/Coordenadoria de Processamento Final/Gerência de Transcrição, 2023. Disponível em: [https://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/RE1037396\\_RE1057258\\_Transcricoes\\_Audiencia\\_Publica\\_38.pdf](https://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/RE1037396_RE1057258_Transcricoes_Audiencia_Publica_38.pdf).

THIERER, Adam. Inovação sem permissão e políticas públicas: um plano de 10 pontos. 2016. p. 11. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2761139](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2761139).

TUFEKCI, Zeynep. Danos algorítmicos além do Facebook e do Google: desafios emergentes da agência computacional. *Colorado Technology Law Journal*, v. 13, 2015, p. 207.

TUTT, Andrew. Uma FDA para algoritmos. *Administrative Law Review*, v. 69, n. 1, 2017.

GOVERNODOREINO UNIDO. Livro Branco sobre Danos Online. 2019. p. 45-46. Disponível em: <https://www.gov.uk/government/consultations/online-harms-white-paper>.

WAGNER, Ben; et al. Regulamentando a Transparência? Facebook, Twitter e a Lei Alemã de Fiscalização de Redes. In: FAT\* '20, 27 a 30 de janeiro, Barcelona, Espanha, 2020, p. 9.

WARDLE, Claire; DERAKHSHAN, Hossein. *DESORDEM DA INFORMAÇÃO: Rumo a uma estrutura interdisciplinar para pesquisa e formulação de políticas*. Relatório do Conselho da Europa, 2017.

WU, Tim. A Inteligência Artificial Vai Devorar o Direito? A Ascensão de Sistemas Híbridos de Ordenação Social. *Columbia Law Review*, v. 119, n. 1, 2019.

ZINGALES, Nicolo. A abordagem brasileira à responsabilidade dos intermediários da Internet: modelo para um regime global? *Internet Policy Review*, v. 4, n. 4, 2015.

# Ataques à democracia no Brasil,

## uma análise da repercussão do 8 de janeiro

Métodos digitais analisam a repercussão da invasão aos Três Poderes da República na Rede Social X

Rita Paulino, Ivone Rocha, Adriano Madureira, Marcos Seruffo

### Resumo

Este artigo apresenta uma pesquisa realizada na rede social X (ex-Twitter) que investiga a repercussão, por esse canal, dos atos de invasão no Congresso Nacional, Supremo Tribunal Federal (STF) e Palácio do Planalto, em Brasília (DF), no dia 8 de janeiro de 2023. O estudo relata métodos digitais diferenciados para entender o contexto do fato investigado desde a coleta de dados com os termos emblemáticos que foram mais divulgados durante as coberturas jornalísticas no Brasil como "Exército", "Terrorismo no Brasil" e "Intervenção". O processo foi dividido em 4 etapas: coleta de dados, Pré-processamento de Dados, Análise Exploratória de Dados, Mapa de tópicos, Identificação de Perfis e Publicações Influentes.

### Introdução

O uso da tecnologia para análise de perfis e discursos em redes sociais tem se mostrado uma ferramenta significativa na compreensão das dinâmicas sociais e políticas. A rede social X, por exemplo, oferece um vasto banco de dados que permite o monitoramento de tendências, a identificação de influenciadores e a análise de padrões de comportamento. No Brasil, essa tecnologia tem sido crucial para

entender como diferentes grupos sociais se mobilizam, propagam mensagens e influenciam o debate público.

Como exemplo, a invasão ao Congresso Nacional (CN), ao Supremo Tribunal Federal (STF) e ao Palácio do Planalto (PP), ocorrida em Brasília no dia 8 de janeiro de 2023, marcou um episódio sem precedentes na história recente do Brasil. Identificados pela mídia como tais, apoiadores do ex-presidente Jair Bolsonaro invadiram as sedes desses Três Poderes, em uma tentativa frustrada de golpe de estado, exigindo a volta do ex-líder ao poder. Com bandeiras, cartazes e slogans inflamados, a multidão promoveu atos de vandalismo e violência, desafiando a ordem democrática do país. A Polícia Militar do Distrito Federal (DF) retomou o controle do prédio do STF após manifestantes furarem bloqueios na Esplanada dos Ministérios.

Uma parte que esse evento de 8 de janeiro complementa é a que recentemente foi investigada e notificada pela Polícia Federal (PF) e pelo STF, em relatório que indiciou 37 pessoas acusadas, incluindo o ex-presidente, com base em levantamentos de provas mais delação premiada, suspeitas de planejar, sem sucesso, o assassinato do recém



eleito, presidente Luiz Inácio Lula da Silva; o vice-presidente, Geraldo Alckmin; e do ministro do STF e então presidente do Tribunal Superior Eleitoral (TSE), Alexandre de Moraes, a partir de 12 de dezembro de 2022. O relatório N° 4546344/2024, 2023.0050897 é público e está disponível no site do STF.

No caso do ataque aos Três Poderes, a invasão intensificou as tensões políticas, levantando preocupações sobre a estabilidade governamental e o Estado Democrático de Direito. Segundo Passeti & Lucato, o evento foi um "desfile destrutivo de legião fascista" (2023, p. 11), sem paralelo nem mesmo com os conflitos políticos dos anos 1930.

Esta pesquisa utiliza o ocorrido no Brasil como um exemplo para demonstrar o uso de métodos digitais na investigação da participação pública nas mídias digitais. A análise de redes sociais (ARS) foi empregada como ferramenta de diagnóstico para tornar explícito o fluxo de informações valiosas que, sendo de outra forma, ficariam ocultas. O estudo focou em palavras e tópicos mais citados nos discursos, buscando entender o contexto, os sentimentos envolventes e as polaridades das postagens. Contempla ainda uma análise qualitativa e quantitativa do comportamento dos perfis que se manifestaram no X (então Twitter, quando realizada a pesquisa), criando uma memória dentro do universo big data.

O trabalho se apoia em estudos que destacam os benefícios dos métodos digitais, técnicas de ARS, como a de sen-

timento e de formação de opinião, na compreensão dos comentários nessas ferramentas. Estudos anteriores, dos quais destacamos os de Chen (2020), Santos (2016) e Mukherjee (2012), ressaltam a importância dessas técnicas na avaliação de comentários online. Mittal (2016) também enfatiza a importância de classificar interesses para otimizar a sobrecarga de informações e melhorar o compartilhamento de recursos nas redes sociais, evidenciando a relevância da ARS em diversas áreas.

Jornalismo orientado por métricas<sup>1</sup> é uma abordagem transformadora na produção de notícias, integrando dados de audiência em todo o fluxo de trabalho. Ele utiliza interações digitais, como cliques e compartilhamentos, para informar decisões, visando quantificar o engajamento e aprimorar a experiência geral das notícias (Wu, 2017). Os princípios-chave incluem incorporar a análise de dados em todos os estágios, priorizar as métricas de interesse do leitor, usar insights para tomada de decisão e empregar algoritmos para curadoria personalizada. Embora prometa maior engajamento, isso levanta preocupações sobre viés de dados, priorizar cliques em detrimento da qualidade e ignorar vozes marginalizadas. A navegação responsável desses desafios enfatizando a ética jornalística, fontes de dados diversas e um compromisso com o jornalismo de qualidade em vez de conteúdo sensacionalista, são princípios fundamentais. Shoemaker & Vos (2015). (Tiwari, S.,2024).

---

1. Metrics-driven journalism is a transformative approach in news production, integrating audience data throughout the workflow. It utilizes digital interactions, such as clicks and shares, to inform decisions, aiming to quantify engagement and enhance the overall news experience (Wu,2017). Key principles include embedding data analysis in all stages, prioritizing reader interest metrics, using insights for decision-making, and employing algorithms for personalized curation. While promising increased engagement, it raises concerns about data bias, prioritizing clicks over quality, and overlooking marginalized voices. Responsible navigation of these challenges is crucial, emphasizing journalistic ethics, diverse data sources, and a commitment to quality journalism over sensationalized content. Shoemaker & Vos (2015).

## Movimentos das redes sociais que se ampliam

As mobilizações de grupos ou coletivos encontram nessas redes um eco importante para a defesa de suas causas. Podemos elencar movimentos como:

- Black Lives Matter, em repúdio à brutalidade policial contra afro-americanos nos Estados Unidos, ilustrada pela revolta ao assassinato de George Floyd, ampliou sua atuação até no Brasil.

- Movimento Me Too, de campanha online contra abuso e assédio sexual às mulheres. Deste surgiram outras campanhas como o Times Up e o Ni Una Menos, ambos também ligados ao mesmo problema (Baker, 2019).

- Movimento por Mudança Climática. Visa a aumentar a conscientização sobre o tema e pressionar autoridades de todo o mundo para a redução das emissões de gases de efeito estufa e nos impactos provocados no clima (Barbi, 2016).

- Movimento por justiça social, abrange diversas causas e direitos de comunidades LGBTQIA+, imigrantes, negros, indígenas e pessoas com deficiência (PCD), para mencionar alguns (Gohn, 2010).

O que todos têm em comum é a abrangência das mobilizações. Avançam no mundo real, com encontros presenciais, eventos nas ruas, em frente a instituições de poder etc. Castells (2013) nos lembra que esses movimentos representam a chave para a transformação social.

De outro lado, há os movimentos da chamada extrema direita, que defendem um nacionalismo e um patriotismo. As grandes mudanças surgem mais para o final do século 20, como um contraponto aos movimentos de luta por democracia, por direitos e contra a ditadura civil-militar. Era a burguesia articulada ao capitalismo inter-

nacional que tinha como propósito diminuir as forças populares (Duarte, 2023). Entre os movimentos de direita, destacamos o nacionalismo extremo, que favorece políticas de limitação de imigração; Autoritarismo, que defende uma forma de governo autoritária e crítica à democracia e aos direitos individuais; Nativismo, oposto à globalização e ao multiculturalismo; Populismo, cuja retórica, envolve as pessoas por meio de emoções e medo (Galeano, 2000).

Foi sob essas bandeiras da extrema-direita que Jair Bolsonaro se elegeu em 2018 para chefiar o Brasil nos quatro anos seguintes (2019-2022), trazendo consigo elementos da dominação de classe. E esses eram os temas representantes da manifestação de ataque à democracia, em 8 de janeiro, com a tentativa de destruição dos Três Poderes do Brasil.

## Técnicas de análise de redes sociais (ARS)

São aplicadas para estudar as interações na plataforma X e compreender os padrões de fala em postagens nas redes sociais. A pesquisa utilizou a Social Network Analysis (SNA) para detectar comunidades sócio semânticas, visualizando tweets como gráficos e calculando frequências de termos (Abascal-Mena *et al.*, 2015). Modelos estatísticos conjuntos foram desenvolvidos para analisar as conexões temáticas entre tweets e transcrições de discurso, revelando que a maioria dos usuários do X fornece feedback de alto nível sobre tópicos gerais, em vez de parágrafos de discurso específicos (Hu *et al.*, 2011).

Uma abordagem de rede multicamadas tem sido empregada para identificar usuários influentes e grupos conectados, com o *PageRank* se mostrando eficaz para classificar a influência individual (Logan *et al.*, 2023).

Paulino & Ventura (2021) observaram que métodos digitais podem revelar comportamentos de rede, de perfis e de sentimentos. A hashtag #Somos70porcento representou uma voz de revolta em um momento de crise sanitária como os vivenciados em 2020 e reforça as mídias sociais como um espaço democrático e de debate.

## Método de pesquisa

A utilização de métodos digitais para análise de conteúdos em escala é cada vez mais relevante, especialmente no contexto da desinformação, pois os jornalistas dependem de ferramentas também digitais para verificação e desenvolvimento de histórias (Beers, 2019). A integração desses recursos no jornalismo local nem sempre é perfeita, alguns lutam para interagir com as suas comunidades através das redes sociais e de dispositivos móveis (Jerónimo, 2020). Apesar desses desafios, a mudança digital

na profissão redefiniu o campo, com o jornalismo digital a tornar-se a norma e não um subcampo (Perreault, 2020).

Esta pesquisa é caracterizada como aplicada e exploratória e teve seu início com a coleta dos dados no então Twitter, em 8 de janeiro, atualmente X. Utilizamos a ferramenta Netlytic para a coleta de dados através de palavras-chaves “Terrorismo no Brasil”, “Intervenção” “Exército”. Termos amplamente divulgados na mídia tradicional para definir o que estava acontecendo naquele dia no Brasil. A Netlytic é uma plataforma de ciência social computacional desenvolvida para executar uma ampla variedade de tarefas centradas em dados, como coletar, analisar e visualizar publicamente aqueles disponíveis de várias plataformas de mídia social (Anatoliy Gruzd *et al.*, 2021). Entretanto, como ela foi descontinuada após a coleta, as demais etapas de análises ocorreram com outros recursos.

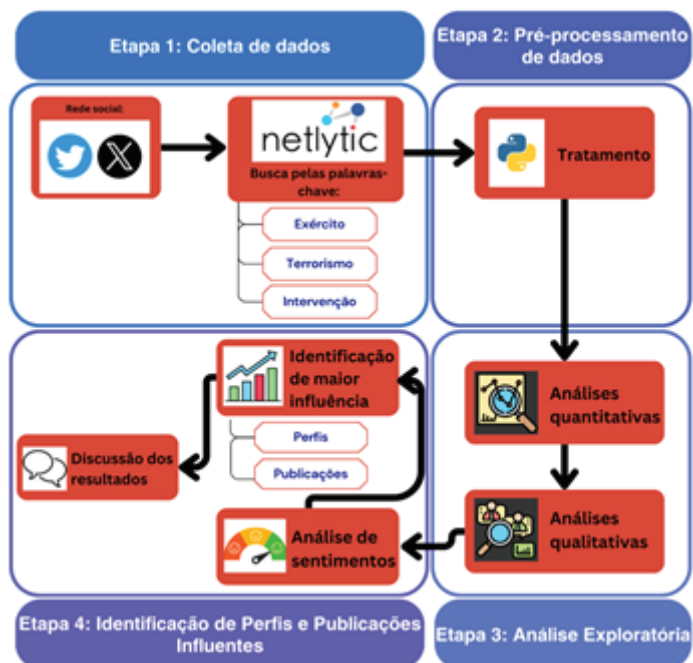
**FIGURA 1. DATASETS COLETADOS COM TERMOS CITADOS PELA MÍDIA.**

	Exército	2023-01-09 07:45:21						<input type="checkbox"/>
	Terrorismo no Brasil	2023-01-09 07:37:44						<input type="checkbox"/>
	Intervenção	2023-01-08 16:47:43						<input type="checkbox"/>

Fonte: Autores/Netlytic

A partir das amostras coletadas (Figura 1), iniciamos uma análise quantitativa e qualitativa para investigar o conteúdo publicado no X e os agentes de publicação. A Figura 2 apresenta um panorama geral do método utiliza-

do, com as etapas do processo, desde a extração e pré-processamento dos dados, passando pela análise exploratória e identificação das métricas de engajamento, até a avaliação dos perfis e publicações influentes.

**FIGURA 2. MÉTODO ADOTADO NA PESQUISA**

Fonte: Autores

### 1. COLETA DE DADOS

Nesta primeira etapa se envolveu a obtenção de informações sobre perfis e publicações influentes da rede social X. A partir dos termos: “Exército”, “Terrorismo” e “Intervenção”, utilizados no período de 8 de janeiro de 2023, foram coletados 10.000 posts em menos de um minuto, com dados que evidenciam a alta participação das pessoas na publicação de suas opiniões sobre o que acontecia.

Os dados foram via “web scraping” (através da plataforma Netlytic), selecionada por permitir a obtenção dessas informações de redes sociais de maneira eficiente. Porém, como a análise foi interrompida pela descontinuidade da plataforma, foi possível a configuração das postagens somente durante o momento da coleta, que compreendeu termos especificados e informações sobre os perfis que os publicaram, incluindo número de seguidores, de tweets e nível de engajamento.

### 2. PRÉ-PROCESSAMENTO DE DADOS

Nesta etapa, os dados coletados são preparados para análise, com a remoção dos duplicados e o tratamento de valores ausentes e de correção de inconsistências. Além disso, houve o processo dos textos para se adequarem à análise dos termos mais frequentes. As palavras foram padronizadas para conter apenas letras minúsculas. Em seguida, símbolos, menções a outros usuários, hashtags e URLs foram removidos para limpeza e foco no conteúdo textual relevante. Abreviaturas comuns foram substituídas por formas completas para facilitar a compreensão e análise dos textos. Por fim, palavras com pouco significado do ponto de vista semântico, conhecidas como stopwords (Ferreira et al., 2023), foram eliminadas dando destaque às mais significativas.

### 3. ANÁLISE EXPLORATÓRIA DE DADOS

Aqui houve uma compreensão inicial dos dados para o cálculo de médias, medianas, desvios-padrão, quartis e percentis sobre eles. Contempla também a visualização de dados por meio de histogramas de frequência para a distribuição das informações coletadas. Com a análise exploratória quantitativa foi possível identificar padrões e anomalias, bem como fornecer um panorama geral das métricas de engajamento. No estudo dos conjuntos de dados por palavra-chave foi possível uma segmentação mais precisa, facilitando a identificação de interesses específicos no contexto do X. As qualitativas ajudaram no melhor entendimento dos conteúdos das publicações e as interações dos usuários. Utilizamos métodos de análise de texto para interpretar o tom e a intenção das postagens.

#### 4. IDENTIFICAÇÃO DE PERFIS E PUBLICAÇÕES INFLUENTES

Nesta etapa, utilizamos métricas relacionadas com o engajamento do usuário em relação ao perfil e às publicações do período. Esse engajamento se relacionou à análise do número de curtidas e compartilhamentos que as publicações de um perfil recebem. E servem para avaliar a visibilidade e a influência de um perfil dentro da rede social (Tufekci, 2013).

As publicações influentes são identificadas com base no engajamento de cada publicação. E servem para fornecer insights sobre os tipos de conteúdo mais eficazes em gerar interação e como as emoções expressas nas postagens impactam o engajamento (Berger; Milkman, 2012). Nas publicações, foram analisados os termos que estão mais relacionados a sinônimos de uma determinada emoção do modelo de Ekman para categorizar aquelas expressas nos tweets (Ekman, 1992).

Na análise qualitativa, incluímos as técnicas de ARS para estudar grafos da amostra coletada com a palavra “Exército”. Utilizamos as métricas do grau de centralidade, a ser abordado mais adiante. Recorremos a esses conceitos visando identificar os perfis mais conectados ou influentes. A centralidade de grau é uma medida das conexões de um ator em uma rede, representando seu potencial para receber ou disseminar informações (Borgatti, 1995).

A partir dos dados coletados na Netlytic, antes de ser descontinuada, exportamos as três bases estudadas no formato CSV para a

ferramenta Communalytic, que proporciona outras análises e visualizações. Nesta pesquisa, utilizamos os recursos de exportação para o formato da ferramenta Gephi, a fim de identificar perfis ativos e influentes.

A escolha da medida de centralidade depende da aplicação específica, da melhoria de atividades de comunicação, da intermediação para controle de comunicação e da proximidade para independência e eficiência. Houve ainda avaliações com base em nuvens de palavras das publicações formadas a partir de um vocábulo central. Elas ajudaram a visualizar os temas mais recorrentes e os verbetes mais importantes dentro das postagens influentes (Viegas; Wattenberg, 2006).

### Análise dos resultados

Como mencionado no tópico da metodologia, analisamos perfis e discursos dos termos pesquisados: “**Terrorismo no Brasil**”, “**Intervenção**” “**Exército**”, palavras que reverberaram nas mídias sociais no dia e após o evento da invasão.

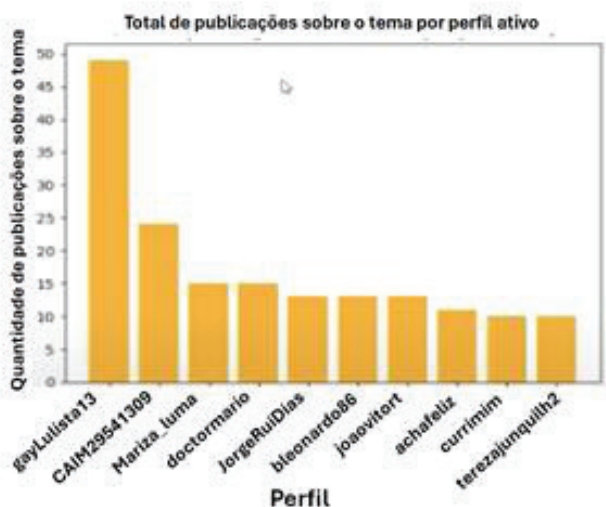
#### ANÁLISE DOS DADOS QUANTITATIVOS

A análise dos dados quantitativos focou em uma abordagem numérica das informações coletadas. Foi possível reunir o total de publicações sobre o tema por perfil ativo, destacando os dez perfis que mais publicaram sobre os temas específicos. Não há uma definição clara sobre o que seja um perfil ativo. Na Rede X entende-se como uma conta que demonstra engajamento regular e significativo com a comunidade.

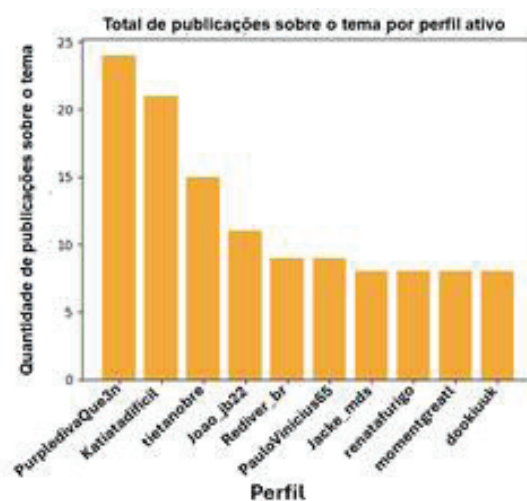
2. O CSV é um formato usado para armazenar dados e que pode ser importado e exportado em programas como Microsoft Excel, Google Sheets, Apple Numbers, OpenOffice Calc e outros aplicativos. Mais informações em: <https://rockcontent.com/br/blog/csv/>

3. software utilizado para estruturação e visualização de redes complexas, tendo em sua base uma infinidade de plug-ins e métricas para a análise de redes, podendo ser utilizado para análise de redes sociais, biológicas entre outras. Mais informações em: [https://files.cercomp.ufg.br/weby/up/771/o/Gephi-Guia\\_B%C3%A1sico\\_de\\_Interface.pdf](https://files.cercomp.ufg.br/weby/up/771/o/Gephi-Guia_B%C3%A1sico_de_Interface.pdf)

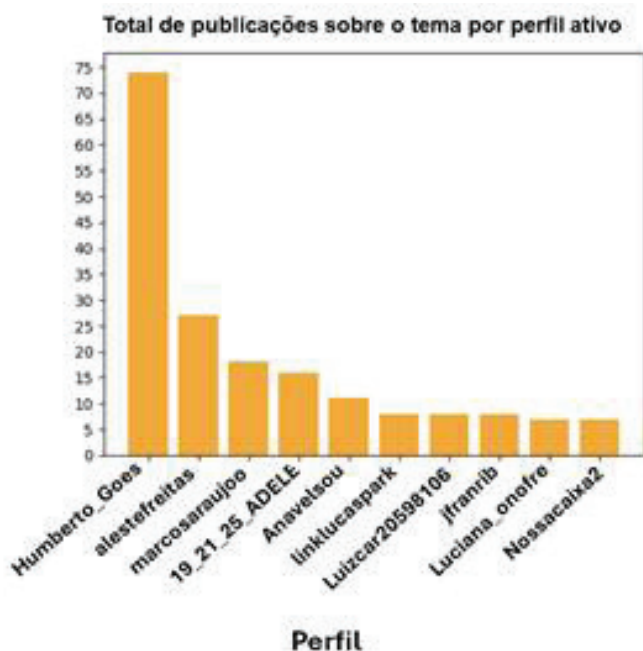
**FIGURA 3. DESTAQUE DOS DEZ PERFIS QUE MAIS PUBLICARAM SOBRE OS TEMAS "EXÉRCITO, INTERVENÇÃO E TERRORISMO (EM ORDEM)"**



**EXÉRCITO**



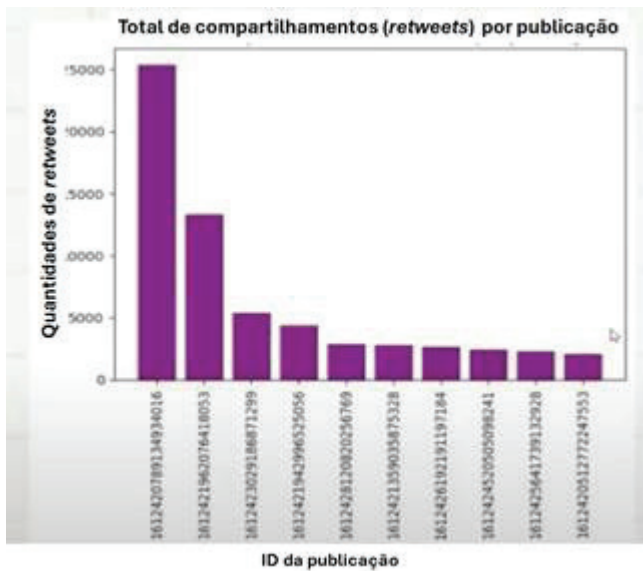
**INTERVENÇÃO**



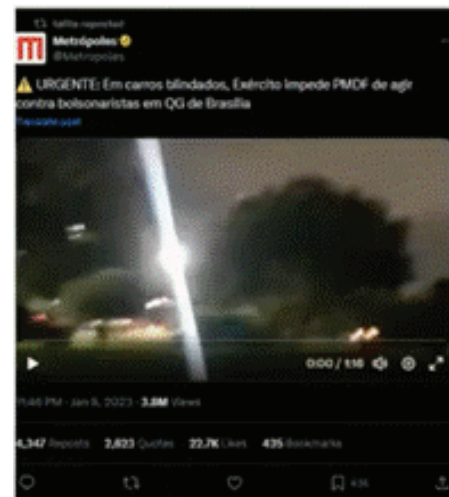
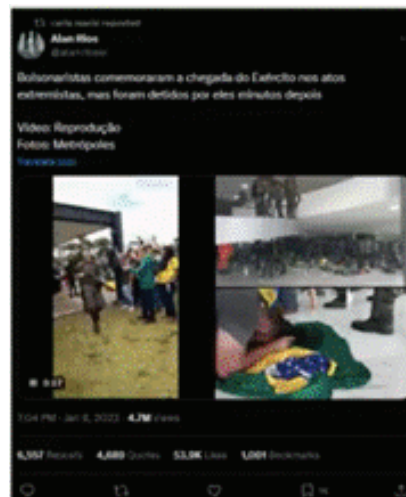
**TERRORISMO**

Essa análise oferece indícios sobre a presença de bots (conhecido como robô, programa de computador projetado para tarefas de forma automatizada, que imita ou substitui ações de um ser humano). Alguns são programados apenas para compartilhar informações, enquanto outros têm a finalidade de disseminar conteúdo. Notamos que alguns usuários ativos fizeram poucas publicações sobre os temas enquanto perfis específicos se destacaram significativamente, como mostrado no início do gráfico, que nos fez suspeitar de bots. Mas isso não se configurou e nos mostrou que esses gráficos permitem uma análise mais precisa e direta, evidenciando a autenticidade e a atividade real do perfil em questão.

## FIGURA 4. PUBLICAÇÕES COM MAIOR NÚMERO DE RETWEETS



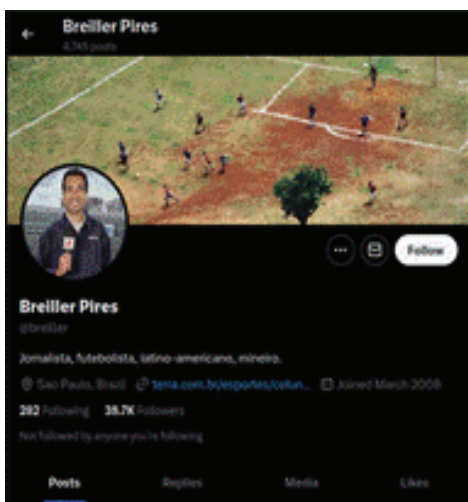
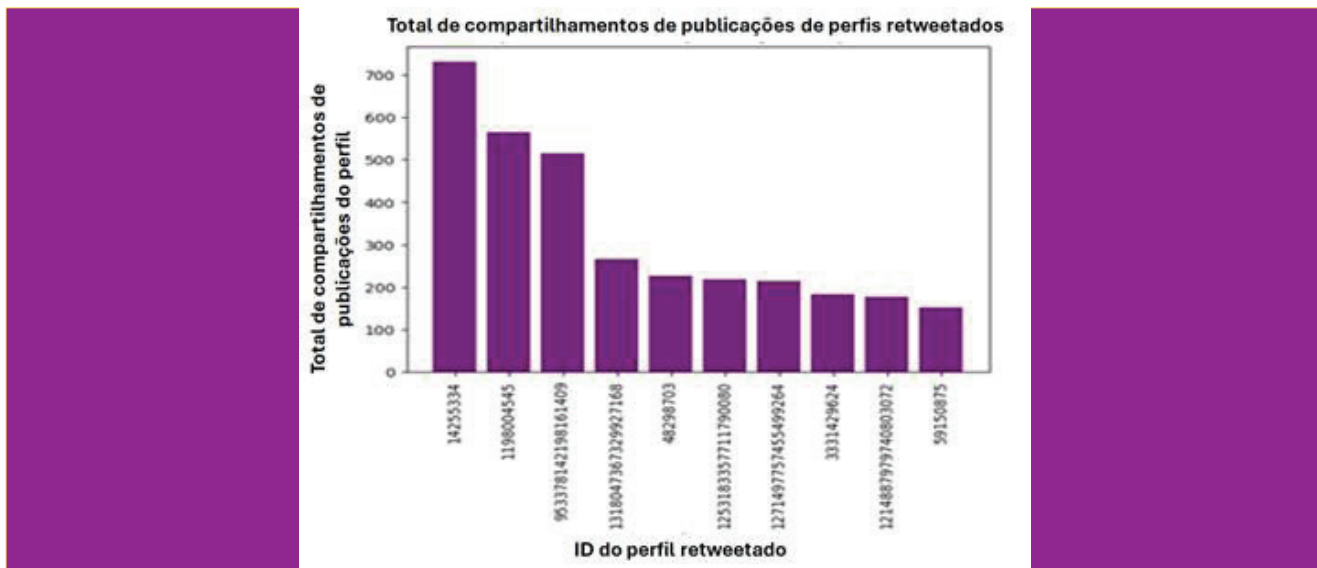
Foram coletadas publicações mais compartilhadas (retweetadas). Ilustramos um exemplo com a coleta do termo “Exército”, selecionando as dez publicações (Figura 4) com maior número de retweets e destacamos as três primeiras do ranking. Igualmente foi feita uma análise da quantidade de retweets por perfil, identificando aqueles com maior número de publicações. Essa análise é acompanhada de capturas de tela ilustrativas.



Fonte: Autores



**FIGURA 5. ANÁLISE DA QUANTIDADE DE RETWEETS POR PERFIL**



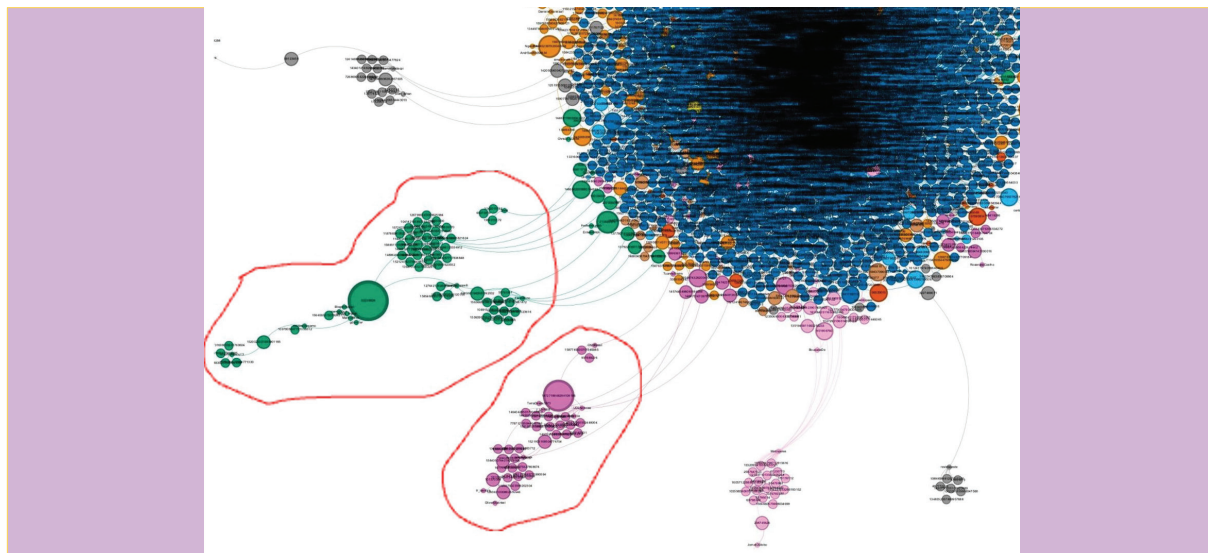
Fonte: Autores

No contexto do processamento de palavras, removemos as "stopwords". Das 10 palavras mais frequentes nos textos originais antes e depois do pré-processamento, observamos termos como "exército", "QG", e "acampamento", que são mais relevantes para a análise. Também

criamos nuvens de palavras (Figura 6) para mostrar os termos mais mencionados nos tweets que contêm as específicas. Por exemplo, a nuvem de palavras para os tweets que mencionam "exército", "intervenção" e "terrorismo" mostram os termos mais relacionados a eles.



**FIGURA 7. GRAFO QUE REPRESENTA AS INTERAÇÕES DA AMOSTRA DE 10.000 TWEETS COLETADAS COM O TERMO “EXÉRCITO”**



Fonte: Visualizado no Gephi/Autores

Além do **cluster maior (Azul)**, os menores do grafo mostram outras conexões ou menções a perfis importantes neste contexto. **O cluster verde**, formado por perfis com alta atividade (elevado *outDegree*<sup>4</sup>), pode representar uma rede de usuários relatando os acontecimentos em tempo real. O quadro 1 (abaixo) apresenta algumas das relações direcionadas por menções.

**Quadro 1. Perfil do cluster verde citando jornalistas ou influenciadores**

Perfil OutDegree	Post	Menções InDegree <sup>5</sup>
63238828	É evidente que isso foi planejado por Bolsonaro! Tem a cara dele! Ato terrorista como a bomba que ele planejou contra o exército quando ainda era militar e foi expulso da corporação! Tá na cara! Não precisa da Inteligência pra chegar a essa conclusão! Tem assinatura! Bolsonaro	@AndreJanonesAdv @monicabergamo @BlogdoNoblat

Fonte: quadro montado pelos autores, a partir do resultado da coleta

4. OutDegree é o grau de saída de um vértice num grafo e representa o tamanho do seu leque de saída, ou seja, o número de arcos que saem do vértice. Mais informações em: [https://www.ime.usp.br/~pf/algoritmos\\_para\\_grafos/aulas/graphs.html](https://www.ime.usp.br/~pf/algoritmos_para_grafos/aulas/graphs.html)

5. O InDegree é o oposto do outDegree, ou seja, é o tamanho do leque de entrada do vértice. Mais informações em: [https://www.ime.usp.br/~pf/algoritmos\\_para\\_grafos/aulas/graphs.html](https://www.ime.usp.br/~pf/algoritmos_para_grafos/aulas/graphs.html)

O **cluster lilás** é similar ao verde, mas com uma estrutura mais dispersa. Indica opiniões e narrativas construídas, com foco em interpretações ou respostas às ações no Planalto.

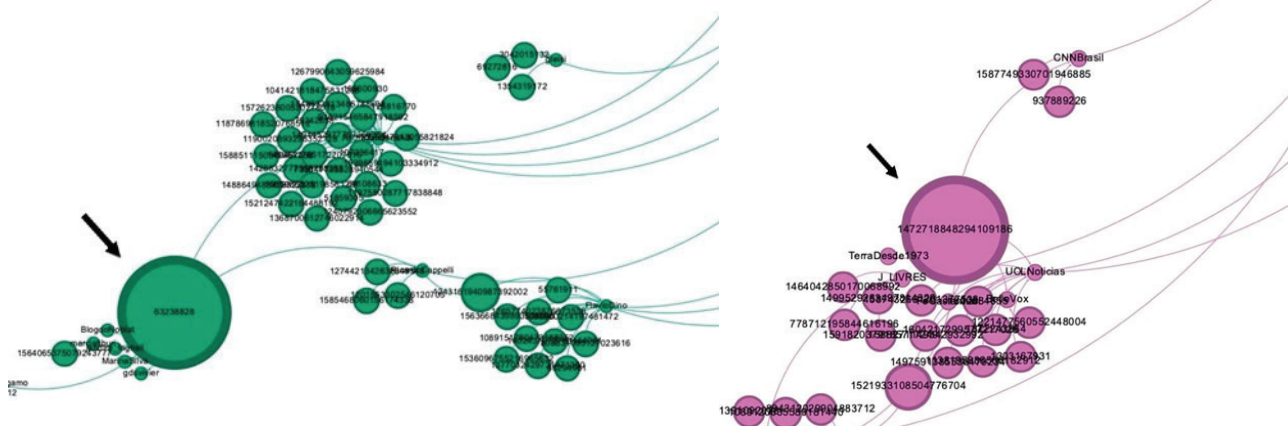
#### Quadro 2. Perfil do cluster verde citando empresas jornalísticas

Perfil OutDegree	Post	Menções InDegree
1472718848294109186	Exército? Qual ? QG do Exército é guardião disso tudo 🤔🤔	@revistaforum @CNNBrasil

Fonte: quadro montado pelos autores, a partir do resultado da coleta

As interligações entre as redes azul, verde e lilás indicam fluxos de informações entre diferentes comunidades. Pode-se inferir que as opiniões e informações cruzavam subgrupos, reforçando ou contradizendo narrativas. Os nós maiores em cada cluster representam perfis com maior engajamento ou atividade.

#### FIGURA 8. GRÁFICO DOS CLUSTERS DESTACADOS NA FIGURA 7



Fonte: Autores

Essa análise visual e estrutural pode ser aprofundada com métricas como grau, modularidade e centralidade para identificar influenciadores e padrões de comunicação no evento. É possível que o caminho de influência transmitido de nós com alto grau e centralidade de proximidade seja semelhante. Ambos podem transmitir rapidamente informações e influência por caminhos diretos

ou curtos para outros e interagir com muitos outros diretamente. (Valente TW, Coronges K, Lakon C, Costenbader E., 2008)

#### ANÁLISE DE CLUSTERS E TÓPICOS

Este é um recurso da ferramenta Communalytic<sup>6</sup>, que descobre tópicos latentes (ou seja, abstratos, que podem não ser observáveis apenas lendo o texto), com base

na similaridade semântica entre postagens (também conhecidas como registros) em um conjunto de dados. O analisador transforma texto em embeddings (vetor de números legível por computador). Uma vez transformados, os textos são agrupados com base em sua similaridade semântica e visualizados por meio de um mapa de similaridade semântica 3D interativo. (Gruzd, A., & Mai, P., 2024).

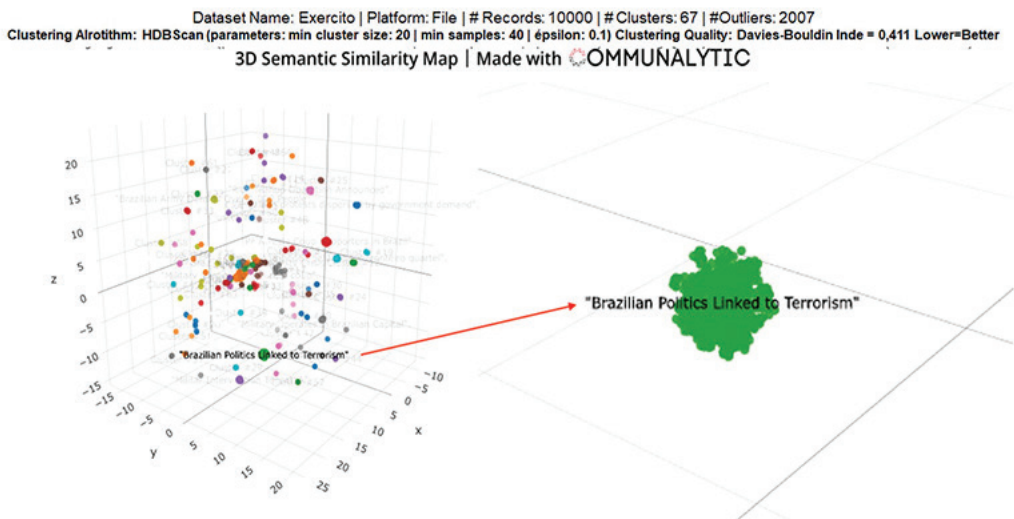
Atualmente, há várias ferramentas para coleta e análise de dados de redes sociais. Muitas delas, principalmente comerciais, como Brandwatch e Talkwalker, apresentam semelhanças significativas entre si e não são adequadas para atender a buscas e coleta de dados para fins de pesquisa em torno de temas específicos. (Carmo I. et al, 2023).

**Quadro 3. Exemplo de diálogo detectado na coleta**

Perfil	Post	Engajamentos
@breiller	<ul style="list-style-type: none"> <li>- Agronegócio: Assassino de povos e comunidades indígenas.</li> <li>- Exército: Covarde e racista.</li> <li>- Pastores evangélicos: Um câncer para tudo que Cristo pregou.</li> <li>- Família Bolsonaro: não consigo nem descrever o meu ódio e meu desejo para eles <a href="https://t.co/H3r5lwaWsN">https://t.co/H3r5lwaWsN</a>.</li> <li>- Agronegócio: Assassino de povos e comunidades indígenas.</li> <li>- Exército: Covarde e racista.</li> <li>- Pastores evangélicos: Um câncer para tudo que Cristo pregou.</li> <li>- Família Bolsonaro: não consigo nem descrever o meu ódio e meu desejo para eles <a href="https://t.co/H3r5lwaWsN">https://t.co/H3r5lwaWsN</a></li> </ul>	<p>@AndreJanonesAdv                  @monicabergamo                  @BlogdoNoblat</p>

Fonte: quadro montado pelos autores, a partir do resultado da coleta

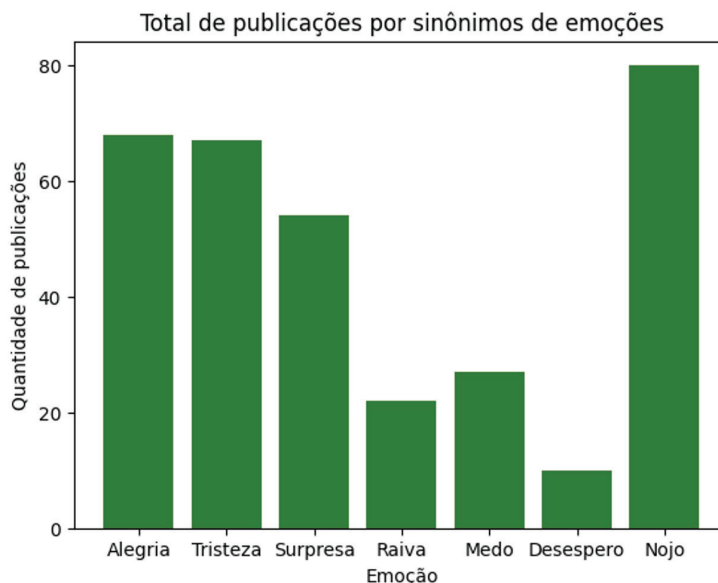
**FIGURA 9. INTERFACE DA PLATAFORMA COMMUNALYTIC APÓS A BUSCA PARA A COLETA**



Fonte: Communalytic

### ANÁLISE DE SENTIMENTOS/ EMOÇÕES

Essa análise se baseia na identificação dos adjetivos utilizados nos textos. E, a partir daqueles presentes nos tweets, conseguimos inferir os sentimentos e emoções expressos. Conforme ilustrado (Figura 10), observamos que o sentimento predominante foi de nojo, seguido por alegria e tristeza, com estes últimos apresentando uma certa equivalência, evidenciando a polaridade emocional dos tweets.



Fonte: Autores

### CONSIDERAÇÕES FINAIS

É possível que o maior desafio das redes sociais digitais esteja em se explorar todas as possibilidades que elas oferecem. Pode ser para melhor compreensão do comportamento humano, por meio de suas ações; para descobrir potencialidades artísticas, culturais, intelectuais; ou até para levantamentos e pesquisas que direcionam ao combate à desinformação, que é o caso deste artigo. Aqui, por meio de pesquisa e análise, mostramos a potencialidade da rede X, em repercutir discursos e narrativas. E quanto mais aumenta a participação popular, mais avolumam-se as ferramentas digitais de levantamento de dados e de análises.

Neste artigo, ao ilustrarmos o evento de 8 de janeiro, envolvendo ataques aos Três Poderes do Estado, tencionamos demonstrar que os métodos digitais de investigação e os resultados obtidos com as técnicas de análise de redes sociais (ARS) contribuem sobremaneira para a compreensão das ações

e das formas de prevenir outras que, porventura, possam vir a desencadear. A adoção de perspectivas práticas para trabalhos futuros pode incluir a implementação de análises automatizadas do discurso. Esta abordagem permitiria a inspeção de amostras textuais e a inferência imediata sobre a veracidade das informações, diferenciando eficazmente entre dados verdadeiros e falsos. No entanto, o principal desafio é lidar com a desinformação, um aspecto que foi abordado nas entrelinhas desta nossa investigação atual. O maior obstáculo que enfrentamos foi a obtenção de um conjunto de dados robusto e representativo, capaz de identificar com precisão o que constitui as chamadas fake news e o que não constitui.

Vimos aqui que grupos se valem das redes sociais para a defesa de suas causas, sejam elas legítimas ou não. Podemos mencionar algumas que, felizmente, encontraram nas redes um canal importante para se fazerem presentes e se estabelecerem na sociedade,

como são os movimentos Black Lives Matter, Me Too, comunidades LGBTQIA+, dos indígenas, para mencionar algumas. Portanto, é essencial que futuras pesquisas se concentrem na análise de conteúdo.

No campo metodológico, utilizamos pesquisa aplicada e exploratória com a análise de dados da rede social X. Foi utilizada na coleta a plataforma Netlytic, que depois de ser desabilitada deu lugar à CommuAnalytic,

para estudar resultados demonstrados em gráficos ilustrativos e imagens, com participação da Inteligência Artificial em referências bem definidas em informações verdadeiras e falsas. As complexidades envolvidas nesse processo exigem um aprofundamento nessas questões e podemos explorar abordagens computacionais viáveis para enfrentar o desafio da desinformação de maneira eficaz e inovadora. ■

**Rita Paulino** é Pós-Doutora, ex-bolsista do CNPq no Social Media Lab na Universidade de Ryerson, Toronto - Ca em 2020. Concluiu o Doutorado no Programa de Pós-Graduação Engenharia e Gestão do Conhecimento, na área de Mídia e Conhecimento, pela Universidade Federal de Santa Catarina em 2011. É professora do curso de Jornalismo e do Programa de Pós-Graduação em Jornalismo (PPGJOR0, ambos da Universidade Federal de Santa Catarina. E-mail: rcpauli@gmail.com.

**Ivone Rocha** é doutoranda pelo Programa de Pós-Graduação em Jornalismo da Universidade Federal de Santa Catarina (PPGJOR/UFSC), estágio em doutoramento pela Universidade de Coimbra, mestre em políticas públicas, especialista em tecnologia da informação e graduada em jornalismo. Integra o grupo de pesquisa CNPQ HiperMídia e Linguagem (Nephi-Jor). E-mail: ivoneasr@gmail.com.

**Adriano Madureira** é doutorando em Engenharia Elétrica, com mestrado e graduação na mesma área pela Universidade Federal do Pará (UFPA). Atualmente exerce pesquisas com foco em Inteligência Computacional, Visão Computacional e Processamento de Linguagem Natural. E-mail: adrianomadureira1@gmail.com.

**Marcos Seruffo** é Doutor em Engenharia Elétrica, com ênfase em Computação Aplicada (PPGEE - UFPA - 2012). Pós-doutorado na Pontifícia Universidade Católica do Rio de Janeiro, no Programa de Pós Graduação em Engenharia Elétrica (PPGEE - PUC-RJ - 2020) . É mestre em Ciências da Computação e graduado em Tecnologia em Processamento de Dados. E-mail: seruffo@ufpa.br.

## Referências

- ABASCAL-MENA, R., LEMA, R. & SÈDES, F. (2015) Detecting sociosemantic communities by applying social network analysis in tweets. *Soc. Netw. Anal. Min.* 5, 38 . <https://doi.org/10.1007/s13278-015-0280-2>.
- ALJOSHA, Karim Schapals (2020 ) Automated journalism: expendable or supplementary for the future of journalistic work? In: Greg Hearn. *The Future of Creative Work*, 99–107. <https://doi.org/10.4337/9781839101106.00014>.
- ALARCÓN, D.M.; ALARCÓN, I.; & ALARCÓN, L.F. (2013). *Social Network Analysis: A Diagnostic tool for information Flow in the AEC Industry*. Disponível em: <https://www.iglc.net/papers/details/864>. Acesso em 19 ago. 2024
- Bakhtin, M. M. *Marxismo e filosofia da linguagem*. São Paulo: Hucitec, 2010.
- BARBI, Fabiana. *Mudanças climáticas e respostas políticas nas cidades*. Campinas-SP: Ed. Unicamp, 2016.
- BAKER, Chandler. *Rede de Sussurros*. Rio de Janeiro: Editora Intrínseca, 2019
- BARROS, C. A.; CHASTINET, A.; PEREIRA, H. B.; SENNA, V. D. Melhorias em medidas de centralidade para difusão em redes complexas, v. X, n. Y, p. XX-YY, mês, 2015.
- BEERS, A. (2019). Examining the digital toolsets of journalists reporting on disinformation. Disponível em: [https://bpb-us-w2.wpmucdn.com/sites.northeastern.edu/dist/d/53/files/2020/02/CJ\\_2020\\_paper\\_50.pdf](https://bpb-us-w2.wpmucdn.com/sites.northeastern.edu/dist/d/53/files/2020/02/CJ_2020_paper_50.pdf). Acesso em 24 ago. 2024.
- BERGER, J.; MILKMAN, K. L. 2012 What makes online content viral? *Journal of Marketing Research*, v. 49, n. 2, p. 192-205.
- BORGATTI, Stephen P. *Centrality and AIDS*. Disponível em: [https://www.researchgate.net/publication/284236341\\_Centrality\\_and\\_AIDS](https://www.researchgate.net/publication/284236341_Centrality_and_AIDS), 1995.
- Carmo, I., L. C. Rêgo, A., Barreto, M., Schuler, M., Heine, A., Villas, M., & Lifschitz, S. (2023). Gerenciamento de Dados de Redes Sociais com Análise de Redes e Modelagem de Tópicos. In *Anais Estendidos do XXXVIII Simpósio Brasileiro de Bancos de Dados*, (pp. 64-70). Porto Alegre: SBC. doi:10.5753/sbbd\_estendido.2023.233417
- CHEN, Cheryl Wei-Yu (2020) Analyzing online comments: a language-awareness approach to cultivating digital literacies, *Computer Assisted Language Learning*, 33:4, 435–454. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/09588221.2019.1569068>. Acesso em 19 ago. 2024.
- CASTELLS, Manuel. *Redes de indignação e esperança: movimentos sociais na era da internet*. Tradução Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013
- DUARTE, Kamilla Alves. Dominação burguesa entre o velho e o novo: a ascensão da extrema-direita no Brasil. *Serv. Soc. Soc.*, São Paulo, v. 146(3), e-6628330, 2023. Disponível em: <https://www.scielo.br/j/ssoc/a/JSQhmDk8n5Q4jbLmVqJnwDy/?format=pdf&lang=pt>. Acesso em: 24 jul. 2024.
- Colina, C.L., Roldán, P.L., Bolívar, M., & Muntanyola, D. (2013). La centralidad en las redes sociales: medición, correlación y aplicación.
- EKMAN, P. (1992) An argument for basic emotions. *Cognition & Emotion*, v. 6, n. 3-4, p. 169-200. Disponível em: <https://www.paulekman.com/wp-content/uploads/2013/07/An-Argument-For-Basic-Emotions.pdf>. Acesso em 19 ago. 2024.
- FERREIRA, Barbara P. J. M.; DALIP, Daniel H.; SILVA, Ismael S. (2023) Análise e Classificação de Gêneros Musicais com Base em Letras de Músicas. In: *SIMPÓSIO BRASILEIRO DE BANCO DE DADOS (SBBB)*, 38. , 2023, Belo Horizonte/MG. *Anais [...]*. Porto Alegre: Sociedade Brasileira de Computação. p. 39-50. ISSN 2763-8979. Disponível em: <https://doi.org/10.5753/sbbd.2023.232425>. Acesso em 24 ago.2024.

- GALEANO, Eduardo. *As veias abertas da América Latina*. Rio de Janeiro: Paz e Terra, 2000
- GOHN, Maria da Glória. *Movimentos sociais*. São Paulo: Vozes, 2010
- GOLDER, S. A.; MACY, M. W. (2011) Diurnal and seasonal mood vary with work, sleep, and daylength across diverse cultures. *Science*, v. 333, n. 6051, p. 1878-1881. Disponível em: <https://pubmed.ncbi.nlm.nih.gov/21960633/>. Acesso em 24 ago. 2024.
- GRUZD, A. (2023). Netlytic: Software for Automated Text and Social Network Analysis. Available at <http://Netlytic.org> Disponível em: [https://netlytic.org/home/?page\\_id=49](https://netlytic.org/home/?page_id=49). Acesso em 24 ago. 2024.
- Gruzd, A., & Mai, P. (2024). Communalytic: A no-code computational social science research tool for studying online communities and public discourse on social media. Available at <https://Communalytic.org>
- HU, Y., JOHN, A., & SELIGMANN, D.D. (2011). Event analytics via social media. *SBNMA '11*. Disponível em: <https://dl.acm.org/doi/abs/10.1145/2531602.2531623>. Acesso em 24 ago. 2024.
- JERÓNIMO, Pedro; CORREIA, João; GRANDIM, Anabela. (2022). Are We Close Enough? Digital Challenges to Local Journalists, *Journalism Practice*, 16:5, 813-827. Disponível em: 10.1080/17512786.2020.1818607. Acesso em 24 ago. 2024.
- LOGAN, A.P., LACASSE, P.M., & LUNDAY, B.J. (2023). Social network analysis of Twitter interactions: a directed multilayer network approach. *Social Network Analysis and Mining*, 13. Disponível em: <https://link.springer.com/article/10.1007/s13278-023-01063-2>. Acesso em 24 ago. 2024.
- LÓPEZ-ROLDÁN, Pedro; COLINA, Claudia L.; PLANAS, Marc B.; SAURA, David M. *La centralidad en las redes sociales*. Barcelona: UOC, 2013.
- KAPLAN, A. M.; HAENLEIN, M. (2010) Users of the world, unite! The challenges and opportunities of social media. *Business Horizons*, v. 53, n. 1, p. 59-68. Disponível em: [https://www.researchgate.net/publication/222403703\\_Users\\_of\\_the\\_World\\_Unite\\_The\\_Challenges\\_and\\_Opportunities\\_of\\_Social\\_Media](https://www.researchgate.net/publication/222403703_Users_of_the_World_Unite_The_Challenges_and_Opportunities_of_Social_Media). Acesso em 24 ago.2024.
- MITTAL, Prathma; GARG, Shivangi and YADAV, Sunita (2016). Social Network Analysis using Interest Mining: A Critical Review. *Indian Journal of Science and Technology*, Vol 9(16). Disponível em: [https://www.researchgate.net/publication/303377102\\_Social\\_Network\\_Analysis\\_using\\_Interest\\_Mining\\_A\\_Critical\\_Review](https://www.researchgate.net/publication/303377102_Social_Network_Analysis_using_Interest_Mining_A_Critical_Review). Acesso em 24 ago.2024
- MUKHERJEE, S. (2012). Identifying the greatest team and captain: A complex network approach to cricket matches. *Physica A: Statistical Mechanics and its Applications*, 391(23), 6066-6076. Disponível em <https://www.sciencedirect.com/science/article/abs/pii/S0378437112006127>. Acesso em 24 ago. 2024.
- THURMAN,Neil; LEWIS, Seth C. & KUNERT, Jessica (2019) Algorithms, Automation, and News, *Digital Journalism*, 7:8, 980-992, DOI: 10.1080/21670811.2019.1685395
- NOAIN-SÁNCHEZ, A. (2022). Addressing the Impact of Artificial Intelligence on Journalism: the perception of experts, journalists and academics. *Communication & Society*, 35(3), 105-121. <https://doi.org/10.15581/003.35.3.105-121>
- PASSETTI, Edson & LUCATO, Diego. (2024) 8 de janeiro de 2023, um golpe de ar azedo. *Publicações UERJ*. Disponível em: <https://www.e-publicacoes.uerj.br/mnemosine/article/view/76206/46043>, acesso em 03 jun.
- PAULINO, Rita de Cássia Romeiro & VENTURA, Mariane Pires,. (2021). O engajamento no Twitter: Métodos de análise para #Somos70porcento. *Cuadernos.info*, (49), 51-71. <https://dx.doi.org/10.7764/cdi.49.27293>
- PERREAULT. Gregory P. & FERRUCCI, Patrick (2020). What Is Digital Journalism? Defining the Practice and Role of the Digital Journalist, *Digital Journalism*, 8:10, 1298-1316. Disponível em: [https://www.researchgate.net/publication/346920686\\_What\\_Is\\_Digital\\_](https://www.researchgate.net/publication/346920686_What_Is_Digital_)

Journalism\_Defining\_the\_Practice\_and\_Role\_of\_the\_Digital\_Journalist. Acesso em 24 ago. 2024.

SANTOS, R. et al , Evaluating the importance of Web comments through metrics extraction and opinion mining, 2016 35th International Conference of the Chilean Computer Science Society (SCCC), Valparaiso, Chile, 2016, pp. 1-11. Disponível em: [https://www.researchgate.net/publication/313452644\\_Evaluating\\_the\\_importance\\_of\\_Web\\_comments\\_through\\_metrics\\_extraction\\_and\\_opinion\\_mining](https://www.researchgate.net/publication/313452644_Evaluating_the_importance_of_Web_comments_through_metrics_extraction_and_opinion_mining). Acesso em 24 ago. 2024.

SCHMIDT, A. L. et al. (2017) Polarization of climate change on Twitter. *Nature Climate Change*, v. 7, n. 3, p. 158-163. Disponível em: [https://www.researchgate.net/publication/273837016\\_Polarized\\_frames\\_on\\_'climate\\_change'\\_and\\_'global\\_warming'\\_across\\_countries\\_and\\_states\\_Evidence\\_from\\_Twitter\\_big\\_data](https://www.researchgate.net/publication/273837016_Polarized_frames_on_'climate_change'_and_'global_warming'_across_countries_and_states_Evidence_from_Twitter_big_data). Acesso em 24 ago. 2024.

SUPREMO TRIBUNAL FEDERAL (STF). Relatório N° 4546344/2024 2023.0050897-Cgcint/Dip/Pf Registro Especial: 2023.0050897-Cgcint/Dip/Pf (Inquérito Policial nº 2021.0044972). Disponível em <https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2024/11/26160436/Relatorio-Final-PF-Site-2024-1.pdf>. Acesso em 20 nov. 2024)

SHIVANI TIWARI, "The Role of Artificial Intelligence in Automated Journalism: Transforming News Production", *International Journal of Creative Research Thoughts (IJCRT)*, ISSN:2320-2882, Volume.12, Issue 5, pp.m799-m838, May 2024, Available at: <http://www.ijcrt.org/papers/IJCRT21X0233.pdf>

TUFEKCI, Z. (2013) Big data: Pitfalls, methods and concepts for an emergent field. *IEEE Annals of the History of Computing*, v. 44, n. 1, p. 55-66. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2229952](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2229952). Acesso em 24 ago. 2024

VIÉGAS, B. F., AND WATTENBERG M., (2008). TIMELINES Tag clouds and the case for vernacular visualization. *interactions* 15, 4 (July + August 2008), 49–52. <https://doi.org/10.1145/1374489.1374501>

Valente, T.W., Coronges, K., Lakon, C.M., & Costenbader, E. (2008). How Correlated Are Network Centrality Measures? *Connections*, 28 1, 16-26 .

.....



# Um balanço do choque do DeepSeek

Publicado originalmente em <https://cyber.fsi.stanford.edu/gdpi/publication/taking-stock-deepseek-shock>

Charles Mok

À medida que a China se aproxima do Ano Novo Lunar, a DeepSeek "entrou em silêncio" no "modo de férias".<sup>1</sup> Com sua sede em Hangzhou deserta, o resto do mundo pondera o choque e a repercussão após o lançamento do modelo de raciocínio de inteligência artificial (IA) R1 e do modelo sem raciocínio V3. Esses modelos têm desempenho equivalente<sup>2</sup> ao modelo de raciocínio o1 e ao GPT-4o da OpenAI, respectivamente, por uma pequena fração do preço.

Em 27 de janeiro de 2025, o mercado de ações dos EUA e as ações de tecnologia sofreram uma das maiores quedas da história,<sup>3</sup> com a fabricante de chips nVidia caindo 18%, perdendo US\$ 589 bilhões em valor de mercado. No entanto, as ações da empresa se recuperaram no dia seguinte em cerca de 9%.<sup>4</sup>

Além da turbulência causada no mercado de ações, as implicações para a atual competição de IA entre os EUA e a China continuam a se desdobrar. Para entender como o DeepSeek impactará o ecossistema global de IA, vamos considerar as cinco perguntas a seguir, com uma pergunta bônus final.

## Como o DeepSeek chegou onde está hoje?

O DeepSeek começou em 2023 como um projeto paralelo<sup>5</sup> do fundador Liang Wenfeng, cuja empresa de fundos de hedge de negociação quantitativa, High-Flyer, utilizava IA para tomar decisões de negociação. Mas Liang começou a acumular milhares de chips nVidia já em 2021. Embora Liang, assim como o DeepSeek, tenham sido relativamente discretos e não tenham dado muitas entrevistas, em um artigo em chinês em julho de 2024,<sup>6</sup> ele discutiu detalhadamente sua visão tecnológica, estratégia e filosofia.

Liang foi um disruptor, não apenas para o resto do mundo, mas também para a China. Sua crença fundamental é que a maioria das empresas chinesas estava simplesmente acostumada a seguir, em vez de inovar, e sua visão era mudar isso. Para ele, o que falta à China e às empresas chinesas não é capital, mas sim confiança e a capacidade de organizar e gerenciar talentos para concretizar verdadeiras inovações.

1. <https://finance.yahoo.com/news/chinese-ai-start-deepseek-breaks-093000108.html>

2. <https://www.exponentialview.co/p/deepseek-everything-you-need-to-know>

3. <https://www.nbcnews.com/business/markets/tech-stocks-react-chinas-deepseek-sparks-us-worries-ai-race-rcna189394>

4. <https://finance.yahoo.com/news/live/stock-market-today-nasdaq-jumps-to-chip-away-at-deepseek-fueled-rout-as-nVidia-surges-nearly-9-210344963.html>

5. <https://fortune.com/2025/01/27/deepseek-founder-liang-wenfeng-hedge-fund-manager-high-flyer-quant-trading/>

6. <https://finance.sina.com.cn/tech/2025-01-26/doc-inehksk9178057.shtml>

Enquanto a maioria das outras empresas chinesas de IA se contenta em "copiar" modelos de código aberto existentes, como o Llama da Meta, para desenvolver suas aplicações, Liang foi além. Seu objetivo final é desenvolver a verdadeira inteligência artificial geral (IAG), a inteligência da máquina capaz de compreender ou aprender tarefas como um ser humano. Ele decidiu concentrar-se no desenvolvimento de novas estruturas de modelos baseadas na realidade da China, com acesso e disponibilidade limitados de chips avançados de processamento de IA.

Os talentos contratados pela DeepSeek eram novos ou recém-formados graduados e doutorandos das principais universidades chinesas. A organização da empresa era plana, e as tarefas eram distribuídas entre os funcionários "naturalmente", moldadas em grande parte pelo que os próprios funcionários queriam fazer. A organização de baixo para cima da DeepSeek como uma startup parecia tão "Vale do Silício" quanto possível, e eles pareciam ter superado seus verdadeiros rivais do Vale do Silício nos EUA em seu próprio jogo. De acordo com benchmarks,<sup>7</sup> o R1 da DeepSeek não apenas iguala a qualidade do OpenAI o1 com um preço 90% mais barato, como também é quase duas vezes mais rápido, embora o o1 Pro da OpenAI ainda forneça respostas melhores.

O sucesso do DeepSeek já pode sinalizar outra nova onda de desenvolvimento tecnológico chinês sob uma bandeira conjunta "pública-privada" de inovação local. Em uma entrevista de Liang<sup>8</sup> ao portal de notícias de tecnologia chinês 36Kr em julho de 2024, ele disse:

*“Acreditamos que a tecnologia de IA da China não seguirá os passos de seus antecessores para sempre. A gigante americana de semicondutores nVidia conseguiu estabelecer sua posição atual não apenas por meio dos esforços de uma única empresa, mas também por meio dos esforços das comunidades e indústrias de tecnologia ocidentais. A indústria chinesa de IA precisa criar esse ecossistema. O desenvolvimento de chips fabricados internamente estagnou na China porque não conta com o apoio das comunidades de tecnologia e, portanto, não consegue acessar as informações mais recentes. É por isso que a China precisa de pessoas na vanguarda da tecnologia.”*

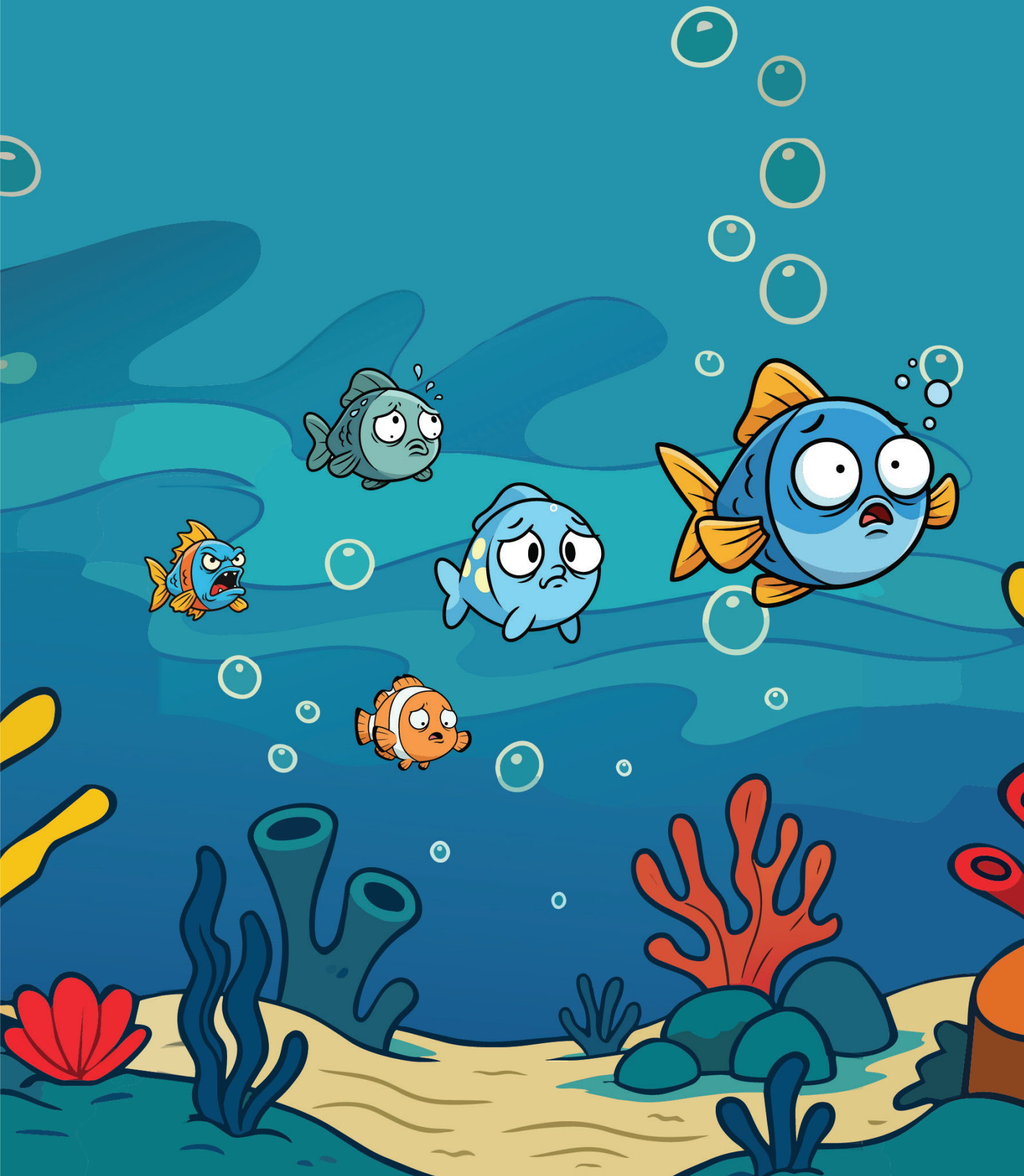
## A DeepSeek realmente gastou menos de US\$ 6 milhões para desenvolver seus modelos atuais?

De acordo com o Relatório Técnico do DeepSeek-V3, publicado pela empresa em dezembro de 2024, os "custos econômicos de treinamento do DeepSeek-V3"<sup>9</sup> foram cobertos por meio de seu "co-design otimizado de algoritmos, estruturas e hardware", utilizando um aglomerado de 2.048 GPUs nVidia H800 para um total de 2.788 milhões de horas de GPU para concluir as etapas de treinamento, desde o pré-treinamento, extensão de contexto e pós-treinamento, para 671 bilhões de parâmetros. O custo total do treinamento de US\$5,576 milhões pressupõe um preço de aluguel de US\$2 por GPU-hora. O relatório técnico observou que esse valor de custo excluiu "os custos associados a pesquisas ante-

7. <https://www.exponentialview.co/p/deepseek-everything-you-need-to-know>

8. <https://asia.nikkei.com/Business/36Kr-KrASIA/DeepSeek-founder-says-China-AI-will-stop-following-U-S>

9. <https://arxiv.org/pdf/2412.19437>



riores e experimentos de ablação em arquiteturas, algoritmos ou dados”.

Deve-se notar que tais parâmetros sobre a quantidade e o tipo específico de chips usados foram projetados para cumprir com os controles de exportação dos EUA lançados em 2022. De acordo com Gregory Allen,<sup>10</sup> diretor do Wadhvani AI Center no Center for Strategic and International Studies (CSIS), o custo total do treinamento poderia ser “muito maior”, já que o valor divulgado cobriu apenas o custo da execução final e bem-sucedida do treinamento, mas não a pesquisa e experimentação anteriores. Além disso, especialistas em IA não identificados também disseram à Reuters que “esperavam que os estágios iniciais de desenvolvimento dependessem de uma quantidade muito maior de chips” e tal investimento “poderia ter custado mais de US\$1 bilhão”.<sup>11</sup> Outra fonte não identificada de uma empresa de IA familiarizada com o treinamento de grandes modelos de IA estimou à Wired que “cerca de 50.000 chips nVidia” foram provavelmente usados.<sup>12</sup>

Compreensivelmente, com as escassas informações divulgadas pela DeepSeek, é difícil tirar conclusões precipitadas e acusar a empresa de subestimar o custo do treinamento e desenvolvimento do V3 ou de outros modelos cujos custos não foram divulgados. A DeepSeek optou por contabilizar o custo do treinamento com base no preço do aluguel do total de horas de GPU, considerando apenas o uso. Não levou em consideração o investimento feito na compra de milhares de modelos diferentes de chips nVidia e outros custos de infraestrutura.

Com base em relatórios divulgados pela empresa, a DeepSeek comprou 10.000 chips nVidia A100, lançados pela primeira vez em 2020 e duas gerações antes do atual chip Blackwell da nVidia, antes que os A100s fossem restringidos para venda na China no final de 2023. A empresa também adquiriu e manteve um cluster de 50.000 nVidia H800s, que é uma versão mais lenta do chip H100 (uma geração antes do Blackwell) para o mercado chinês.

A DeepSeek provavelmente também tinha acesso ilimitado adicional a provedores de serviços de nuvem chineses e estrangeiros,<sup>13</sup> pelo menos antes que estes últimos fossem submetidos aos controles de exportação dos EUA. Mesmo que a empresa não tenha divulgado sua participação em mais chips nVidia, apenas os 10.000 chips nVidia A100 custariam perto de US\$80 milhões, e 50.000 H800s custariam US\$50 milhões adicionais.

Em outras palavras, comparar uma pequena parcela do custo do tempo de uso do treinamento de IA autodeclarado pela DeepSeek com o investimento total em infraestrutura para aquisição de chips de GPU ou construção de datacentros por grandes empresas de IA dos EUA não é uma comparação justa nem direta. Além disso, essa infraestrutura não é usada apenas para o treinamento inicial dos modelos — ela também é usada para inferência,<sup>14</sup> onde um modelo de aprendizado de máquina treinado tira conclusões de novos dados, normalmente quando o modelo de IA é usado em uma situação de usuário para responder a consultas.

10. <https://asia.nikkei.com/Business/Technology/Artificial-intelligence/nVidia-killer-or-overhyped-4-things-to-know-about-China-s-DeepSeek2>

11. <https://www.reuters.com/technology/artificial-intelligence/american-ai-firms-try-poke-holes-disruptive-deepseek-2025-01-28/>

12. <https://www.wired.com/story/deepseek-executives-reaction-silicon-valley/>

13. <https://www.chinatalk.media/p/deepseek-what-the-headlines-miss>

14. <https://www.cloudflare.com/learning/ai/inference-vs-training/>

Embora não haja evidências substanciais atuais para contestar as alegações de custo da DeepSeek, trata-se, no entanto, de uma afirmação unilateral de que a empresa optou por relatar seus custos de forma a maximizar a impressão de ser "a mais econômica". Apesar de a DeepSeek não ter contabilizado seu investimento total real, é sem dúvida uma conquista significativa o fato de ter conseguido treinar seus modelos para que estivessem no mesmo nível de alguns dos modelos mais avançados existentes. Sua otimização e engenharia inovadoras contornaram recursos de hardware limitados, mesmo com relatórios imprecisos de economia de custos.

## O que ditará o futuro do desenvolvimento, dimensionamento ou otimização mais inovadora da IA?

O ditado "a necessidade é a mãe de todas as invenções" existe há séculos.<sup>15</sup> Diante das atuais restrições dos EUA à exportação de produtos e serviços de tecnologia para a China, este país assumiu a urgência resultante da escassez para intensificar seu foco e acelerar seus esforços de desenvolvimento.

Compare o cenário chinês com a indústria de IA dos EUA, que já é dominada por Big Techs e "hectocorns"<sup>16</sup> bem financiadas, como a OpenAI. Com uma avaliação que já ultrapassa US\$ 100 bilhões, a inovação em IA tem se concentrado na construção de uma infraestrutura maior, utilizando os chips de GPU mais recentes e rápidos, para alcançar uma escala cada vez maior por meio de força bruta, em vez de otimizar os algoritmos de treinamento e inferência

para conservar o uso desses recursos computacionais caros. As Big Techs e seus investidores aderem à mesma mentalidade "grande e maior", em busca de avaliações cada vez maiores e um ciclo autorrealizável de vantagens competitivas e retornos financeiros percebidos. Culturalmente, alguns argumentam que mesmo as recentes "startups fragmentadas e disruptivas", como a OpenAI há alguns anos, já "amadureceram e se tornaram o tipo de empresa grande e conectada que é pega de surpresa por rivais que se movem mais rápido".<sup>17</sup>

O que torna o DeepSeek particularmente interessante e verdadeiramente disruptivo é que ele não apenas alterou a economia do desenvolvimento de IA para a indústria de IA dos EUA e seus investidores, mas também já fez o mesmo com suas contrapartes chinesas de IA. Quando o DeepSeek-V2 foi lançado em junho de 2024, de acordo com o fundador Liang Wenfeng,<sup>18</sup> desencadeou uma guerra de preços com outras Big Techs chinesas, como ByteDance, Alibaba, Baidu, Tencent, bem como startups de IA maiores e mais bem financiadas, como a Zhipu AI. Por outro lado, em comparação com a incursão da Huawei no desenvolvimento de produtos e tecnologias de semicondutores, que muitas vezes é considerada apoiada pelo governo, parece improvável que a ascensão do DeepSeek tenha sido planejada de forma semelhante pelo governo.

Nos EUA, ao contrário da forte reação do mercado de ações, a resposta política ao DeepSeek foi bastante contida. O presidente Donald Trump o chamou de "um alerta para nossas indústrias de que precisamos nos concentrar totalmente na competição".<sup>19</sup> Ele

15. <https://hbr.org/2011/03/necessity-not-scarcity-is-the>

16. A hectocorn is a financial term for a company, often a tech startup, valued at over \$100 billion. The name combines the Greek prefix "hecto-" (meaning one hundred) with "unicorn" (a privately held startup valued at over \$1 billion). These are also known as "super-unicorns" and represent a rare level of success and valuation. Source: <https://www.dictionary.com/e/tech-science/hectocorn/>

17. <https://www.politico.com/newsletters/digital-future-daily/2025/01/28/china-out-innovates-the-innovators-00201058>

18. <https://finance.sina.com.cn/tech/2025-01-26/doc-inehksk9178057.shtml>

19. <https://www.nbcnews.com/tech/innovation/trump-china-deepseek-ai-wake-call-rcna189526>

também disse que considerava o DeepSeek "um desenvolvimento muito positivo", porque "em vez de gastar bilhões e bilhões, você gastará menos e, com sorte, chegará à mesma solução".

Há boas razões para Trump ser prudente em sua resposta. Poucos dias após revogar<sup>20</sup> a Ordem Executiva 14110,<sup>21</sup> de 30 de outubro de 2023, do governo anterior (Desenvolvimento e Uso Seguro, Protegido e Confiável de Inteligência Artificial), a Casa Branca anunciou o projeto de infraestrutura de IA Stargate,<sup>22</sup> de US\$500 bilhões, com a OpenAI, Oracle e SoftBank. A indústria americana não poderia, e não deveria, mudar repentinamente de ideia sobre a construção dessa infraestrutura, mas atenção maior deveria ser dada à verificação da validade a longo prazo das diferentes abordagens de desenvolvimento.

A longo prazo, uma vez que a implantação e a adoção generalizadas de aplicações de IA sejam alcançadas, é evidente que os EUA e o mundo ainda precisarão de mais infraestrutura. Alguns analistas de mercado apontaram<sup>23</sup> para o Paradoxo de Jevons,<sup>24</sup> uma teoria econômica que afirma que "o aumento da eficiência no uso de um recurso frequentemente leva a um maior consumo geral desse recurso". Isso não significa que a indústria não deva, ao mesmo tempo, desenvolver medidas mais inovadoras para otimizar o uso de recursos dispendiosos, de hardware a energia.

## Qual será o impacto político nas restrições de exportação de chips avançados dos EUA para a China?

Em comparação com a rápida revogação do decreto do ex-presidente Joe Biden sobre IA, o presidente Trump não abordou a questão das atuais restrições à exportação de chips semicondutores avançados e outros equipamentos industriais avançados para a China. É provável que o novo governo ainda esteja elaborando sua narrativa para uma "nova política", que o diferencie do governo Biden, enquanto mantém essas restrições. É claro que também existe a possibilidade de Trump estar reavaliando essas restrições à exportação no contexto mais amplo de todo o relacionamento com a China, incluindo comércio e tarifas.

A DeepSeek agora impõe nova urgência ao governo para que se posicione sobre os controles de exportação. Se as empresas chinesas ainda conseguem acessar recursos de GPU para treinar seus modelos, a ponto de qualquer uma delas conseguir treinar e lançar com sucesso um modelo de IA altamente competitivo, os EUA deveriam redobrar essas restrições à exportação? Como as restrições à exportação tendem a incentivar a inovação chinesa por necessidade, os EUA deveriam mudar e remover esses controles, permitindo que empresas americanas como a nVidia lucrem com as vendas para a China?

Em primeiro lugar, o fato de a DeepSeek ter conseguido acessar chips de IA não indica uma falha nas restrições à exportação, mas

20. <https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/>

21. <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>

22. <https://www.cnn.com/2025/01/21/tech/openai-oracle-softbank-trump-ai-investment/index.html>

23. <https://asia.nikkei.com/Business/Technology/Artificial-intelligence/nVidia-killer-or-overhyped-4-things-to-know-about-Chinas-DeepSeek2>

24. [https://en.wikipedia.org/wiki/Jevons\\_paradox](https://en.wikipedia.org/wiki/Jevons_paradox)

indica o efeito de atraso na implementação dessas políticas e a natureza gato-e-rato dos controles de exportação. A DeepSeek adquiriu os chips H800 da nVidia para treinamento, e esses chips foram projetados para contornar os controles originais de outubro de 2022.

Restrições adicionais um ano depois fecharam essa brecha, de modo que os chips H20 agora disponíveis que a nVidia agora pode exportar para a China não funcionam tão bem para fins de treinamento.<sup>25</sup> No entanto, de acordo com observadores da indústria,<sup>26</sup> esses H20s ainda permitem implantação de IA de ponta, incluindo inferência, e sua disponibilidade para a China ainda é uma questão a ser abordada.

Apesar dessas deficiências, a lacuna computacional entre os EUA e a China continuaria a aumentar devido aos controles de exportação, um fato citado pela DeepSeek como sua principal limitação. A empresa reconheceu uma desvantagem computacional de 4x, apesar dos ganhos de eficiência, conforme relatado pela ChinaTalk.<sup>27</sup> Para que os EUA mantenham essa liderança, os controles de exportação ainda são uma ferramenta inevitável que vai ser mantida e fortalecida.

Os primeiros indícios indicam que o governo Trump está considerando restrições adicionais às exportações de chips nVidia para a China, de acordo com uma reportagem da Bloomberg,<sup>28</sup> com foco em uma possível proibição dos chips H20s, uma versão reduzida para o mercado chinês. No entanto, a fonte também acrescentou que uma decisão rápida é improvável, já que o indicado de Trump para

Secretário de Comércio, Howard Lutnick, ainda não foi confirmado pelo Senado, e o Departamento de Comércio está apenas começando a receber pessoal. Ese atraso pode significar que, assim como antes, a China pode estocar quantos H20s puder, e pode-se ter certeza de que o fará.

No entanto, no lado oposto do debate sobre as restrições à exportação para a China, há também a crescente preocupação com as tarifas impostas por Trump às importações de chips de Taiwan. No ano passado, as exportações de Taiwan para os EUA<sup>29</sup> aumentaram 46%, para US\$111,3 bilhões, com as exportações de equipamentos de informação e comunicação — incluindo servidores de IA e componentes como chips — totalizando US\$67,9 bilhões, um aumento de 81%. Esse aumento pode ser parcialmente explicado pelo que costumava ser as exportações de Taiwan para a China, que agora são fabricadas e reexportadas diretamente de Taiwan.

Em um discurso no mesmo dia da queda da bolsa de valores devido às notícias sobre o DeepSeek, Trump discursou na Convenção de Questões Republicanas da Câmara<sup>30</sup> e reclamou das empresas "que nos abandonaram e foram para Taiwan", e disse que aplicaria tarifas de até 100%<sup>31</sup> "sobre a produção estrangeira de chips de computador, semicondutores e produtos farmacêuticos para retornar a produção desses bens essenciais aos Estados Unidos".<sup>32</sup>

Se isso realmente acontecer, prejudicará gravemente empresas americanas como AMD, Apple, nVidia e Qualcomm, que com-

25. <https://epoch.ai/gradient-updates/us-export-controls-china-ai>

26. <https://www.chinatalk.media/p/deepseek-what-the-headlines-miss>

27. <https://www.chinatalk.media/p/deepseek-ceo-interview-with-chinas?ref=blog.heim.xyz>

28. [https://www.bloomberg.com/news/articles/2025-01-29/trump-officials-discuss-tightening-curbs-on-nVidia-china-sales?utm\\_source=stack&utm\\_medium=email](https://www.bloomberg.com/news/articles/2025-01-29/trump-officials-discuss-tightening-curbs-on-nVidia-china-sales?utm_source=stack&utm_medium=email)

29. <https://asia.nikkei.com/Economy/Trade/AI-demand-lifts-Taiwan-s-U.S.-exports-investments-to-record-highs>

30. <https://www.c-span.org/program/white-house-event/president-trump-addresses-house-republican-issues-conference/655005>

31. <https://www.newsweek.com/donald-trump-taiwan-semiconductor-tariff-impact-china-tech-2022564>

32. <https://www.pcmag.com/news/trump-to-tariff-chips-made-in-taiwan-targeting-tsmc>

pram da TSMC de Taiwan e outras. Essas empresas irão transferir o custo para seus compradores e consumidores finais. Para a indústria de IA dos EUA, isso não poderia vir em pior momento e pode representar mais um golpe em sua competitividade.

Embora a retomada da indústria manufatureira nos EUA leve anos para ser concretizada, mesmo com as políticas corretas, a imposição de tarifas excessivas pode prejudicar o setor e causar inflação imediata. Seria de se esperar que a retórica de Trump fosse apenas parte de sua habitual estratégia para obter concessões do outro lado. De fato, o premiê de Taiwan, Cho Jung-tai, respondeu aos comentários de Trump,<sup>33</sup> afirmando que o governo consideraria urgentemente a criação de mais planos de cooperação e programas futuros de assistência ao setor industrial.

## Há preocupações sobre a transferência de dados, segurança e desinformação do DeepSeek?

Isaac Stone Fish, CEO da empresa de dados e pesquisa Strategy Risks, disse em sua postagem no X que "a censura e a propaganda no DeepSeek são tão difundidas e tão pró-Partido Comunista que fazem o TikTok parecer uma coletiva de imprensa do Pentágono".<sup>34</sup> De fato, com o hype do DeepSeek impulsionando seu aplicativo para o primeiro lugar na App Store da Apple para aplicativos gratuitos nos EUA e em 51 outros países,<sup>35</sup> o DeepSeek rapidamente se tornou o TikTok para aqueles que se consideram tecnicamente experientes e "sabem o que estão fazendo".

A DeepSeek não esconde que envia dados dos EUA e de outros países para a China. Sua política de privacidade afirma explicitamente: "As informações pessoais que coletamos de você podem ser armazenadas em um servidor localizado fora do país onde você reside. Armazenamos as informações que coletamos em servidores seguros localizados na República Popular da China".<sup>36</sup> Em seus termos de uso, também afirma claramente: "O estabelecimento, a execução, a interpretação e a resolução de disputas sob estes Termos serão regidos pelas leis da República Popular da China continental".<sup>37</sup>

Que tipos de dados podem estar em risco? Além de todas as conversas e perguntas que um usuário envia ao DeepSeek, bem como as respostas geradas, a revista Wired resumiu três categorias de informações que o DeepSeek pode coletar sobre os usuários:<sup>38</sup> informações que os usuários compartilham com o DeepSeek, informações que ele coleta automaticamente e informações que pode obter de outras fontes. Essas informações incluem informações pessoais fornecidas pelos usuários durante o cadastro, as entradas e solicitações de texto ou áudio dos usuários, todos os arquivos enviados, histórico de bate-papo e rastreamento de teclas digitadas, etc.

Como costuma acontecer, a coleta e o armazenamento de muitos dados resultarão em vazamentos. A empresa de segurança em nuvem Wiz Research descobriu recentemente um "banco de dados exposto vazando informações confidenciais, incluindo histórico de bate-papo" do DeepSeek, com mais de um milhão de linhas de registros com "informa-

33. <https://www.cnn.com/2025/01/28/business/trump-tariff-taiwan-chips-intl-hnk/index.html>

34. <https://x.com/isaacstonefish/status/1884232028763349470>

35. <https://techcrunch.com/2025/01/27/deepseek-displaces-chatgpt-as-the-app-stores-top-app/>

36. <https://platform.deepseek.com/downloads/DeepSeek%252520Privacy%252520Policy.html>

37. [https://cdn.deepseek.com/policies/en-US/deepseek-terms-of-use.html?locale=en\\_US](https://cdn.deepseek.com/policies/en-US/deepseek-terms-of-use.html?locale=en_US)

38. <https://www.wired.com/story/deepseek-ai-china-privacy-data/>

ções altamente confidenciais".<sup>39</sup> A empresa informou o DeepSeek, que "imediatamente bloqueou a exposição".

Outra área de preocupação, semelhante à situação do TikTok, é a censura. Vários relatórios indicaram que a DeepSeek evita discutir tópicos políticos chineses sensíveis, com respostas como "Desculpe, isso está além do meu escopo atual. Vamos falar sobre outra coisa".<sup>40</sup> Isso não deveria ser uma surpresa, já que a DeepSeek, uma empresa chinesa, deve aderir a inúmeras regulamentações chinesas que afirmam que todas as plataformas não devem violar os "valores socialistas fundamentais" do país, incluindo o documento "Requisitos básicos de segurança para serviço de inteligência artificial generativa".<sup>41</sup> As empresas são obrigadas a conduzir revisões de segurança e obter aprovações antes que seus produtos possam ser lançados.

O criador de ferramentas de segurança de IA Promptfoo testou e publicou um conjunto de dados de avisos cobrindo tópicos sensíveis que provavelmente seriam censurados pela China e relatou que a censura do DeepSeek parecia ser "aplicada por força bruta" e, portanto, é "fácil de testar e detectar".<sup>42</sup> Ele também expressou preocupação com o uso de dados do usuário pelo DeepSeek para treinamento futuro.

Além das preocupações com os usuários que utilizam diretamente os modelos de IA da DeepSeek, executados em seus próprios servidores, presumivelmente na China e regidos pelas leis chinesas, o que dizer da crescente lista de desenvolvedores de IA fora da China, incluindo os EUA, que adotaram diretamente o serviço da DeepSeek ou hospedaram suas próprias versões dos modelos de código aberto da empresa?

A empresa de busca de IA Perplexity, por exemplo, anunciou a adição dos modelos da DeepSeek à sua plataforma e informou aos seus usuários que seus modelos de código aberto DeepSeek são "completamente independentes da China" e estão hospedados em servidores em datacenters nos EUA e em países da UE.

De acordo com a empresa de segurança cibernética Ironscales, mesmo a implantação local do DeepSeek pode não ser totalmente segura.<sup>43</sup> Primeiro, sem uma auditoria completa do código, não é possível garantir que a telemetria oculta, ou seja, os dados enviados de volta ao desenvolvedor, sejam completamente desativados. A proteção de dados confidenciais também depende da configuração adequada do sistema e de sua proteção e monitoramento contínuos e eficazes. Em outras palavras, é difícil determinar a ausência de "backdoors" sem uma análise mais completa, o que leva tempo. Além disso, há também a questão de se a censura do DeepSeek pode persistir em uma versão murada de seu modelo.

A atual onda de entusiasmo não apenas por usuários casuais, mas também por empresas de IA em todo o mundo, para integrar o DeepSeek rapidamente, pode representar riscos ocultos para muitos usuários que utilizam diversos serviços sem sequer saber que o utilizam. Para que os desenvolvedores possam "experimentar com segurança", o DeepSeek-R1 já está disponível como uma prévia do microsserviço nVidia NIM. Da mesma forma, ele também está disponível no catálogo de modelos do Azure AI Foundry e do GitHub da Microsoft, e a Microsoft afirma ter submetido o DeepSeek-R1 a "avaliações rigo-

39. <https://www.wiz.io/blog/wiz-research-uncovers-exposed-deepseek-database-leak>

40. <https://time.com/7210499/deepseek-r1-chatgpt-china-politics/>

41. <https://www.tc260.org.cn/upload/2024-03-01/1709282398070082466.pdf>

42. <https://www.promptfoo.dev/blog/deepseek-censorship/>

43. <https://ironscales.com/blog/deepseek-ai.-what-it-security-leaders-need-to-know>

rosas de segurança e red teaming, incluindo avaliações automatizadas do comportamento do modelo e extensas revisões de segurança para mitigar riscos potenciais”.

Mas para usuários casuais, como aqueles que baixam o aplicativo DeepSeek em lojas de aplicativos, os riscos e danos potenciais permanecem altos. Testes mostraram que, em comparação com outros modelos de IA dos EUA, é relativamente fácil contornar as proteções do DeepSeek para escrever código que ajude hackers a extrair dados, enviar e-mails de phishing e otimizar ataques de engenharia social, de acordo com a empresa de segurança cibernética Palo Alto Networks.<sup>44</sup> Outra empresa de segurança, a Enkrypt AI, relatou que o DeepSeek-R1 tem quatro vezes mais probabilidade de “escrever malware e outros códigos inseguros do que o o1 da OpenAI”.<sup>45</sup> Um pesquisador sênior de IA da Cisco comentou que o desenvolvimento de baixo custo do DeepSeek pode ter negligenciado sua segurança durante o processo.

Além disso, de acordo com a empresa de confiabilidade de informações NewsGuard, o chatbot do DeepSeek “respondeu aos prompts avançando desinformação estrangeira 35% das vezes” e “60% das respostas, incluindo aquelas que não repetiram a falsa alegação, foram enquadradas da perspectiva do governo chinês, mesmo em resposta a prompts que não fizeram nenhuma menção à China”.<sup>46</sup> De acordo com relatos, o Diretor Administrativo da Câmara dos Representantes dos EUA já emitiu um aviso aos escritórios do Congresso de que “o DeepSeek

está sob revisão pelo CAO e atualmente não está autorizado para uso oficial da Câmara”.<sup>47</sup>

Qual é a posição do presidente Trump em relação à importância dos dados coletados e transferidos para a China pelo DeepSeek? Recentemente, em comentários sobre o TikTok, Trump minimizou as potenciais ameaças à segurança nacional dos EUA, duvidando da importância “da China espionar jovens, crianças assistindo a vídeos malucos”.<sup>48</sup> Será que ele será tão tolerante com o DeepSeek quanto com o TikTok, ou verá níveis mais elevados de riscos pessoais e à segurança nacional que um modelo de IA pode representar?

Por outro lado, os reguladores europeus já estão agindo porque, ao contrário dos EUA, possuem leis de proteção de dados pessoais e privacidade. O regulador italiano de privacidade lançou uma investigação sobre o DeepSeek para verificar se o Regulamento Geral de Proteção de Dados (RGPD) da União Europeia é respeitado.<sup>49</sup> Dado que o DeepSeek admite abertamente que dados de usuários são transferidos e armazenados na China, é muito possível que seja considerado uma violação dos princípios do RGPD. De fato, o aplicativo DeepSeek foi prontamente removido das lojas de aplicativos da Apple e do Google na Itália um dia depois,<sup>50</sup> embora o regulador do país não tenha confirmado se o órgão ordenou a remoção. Separadamente, a agência irlandesa de proteção de dados também lançou sua própria investigação sobre o processamento de dados do DeepSeek.<sup>51</sup>

44. <https://unit42.paloaltonetworks.com/jailbreaking-deepseek-three-techniques/>

45. [https://cdn.prod.website-files.com/6690a78074d86ca0ad978007/679bc2e71b48e423c0ff7e60\\_1%2520RedTeaming\\_DeepSeek\\_Jan29\\_2025%2520\(1\).pdf](https://cdn.prod.website-files.com/6690a78074d86ca0ad978007/679bc2e71b48e423c0ff7e60_1%2520RedTeaming_DeepSeek_Jan29_2025%2520(1).pdf)

46. <https://www.newsguardtech.com/special-reports/deepseek-ai-chatbot-china-russia-iran-disinformation/>

47. <https://www.axios.com/2025/01/30/house-congress-bans-deepseek-ai>

48. <https://abcnews.go.com/US/trump-questions-concerns-tiktok-important-current-former-aides/story?id=118036458>

49. [https://www.politico.eu/article/italys-privacy-regulator-goes-after-deepseek/?utm\\_source=substack&utm\\_medium=email](https://www.politico.eu/article/italys-privacy-regulator-goes-after-deepseek/?utm_source=substack&utm_medium=email)

50. <https://www.reuters.com/technology/deepseek-app-unavailable-apple-google-app-stores-italy-2025-01->

51. [https://www.reuters.com/technology/irish-data-regulator-requests-information-deepseek-data-processing-2025-01-29/?utm\\_source=substack&utm\\_medium=email](https://www.reuters.com/technology/irish-data-regulator-requests-information-deepseek-data-processing-2025-01-29/?utm_source=substack&utm_medium=email)

## O DeepSeek trapaceou?

Nos dias que se seguiram ao lançamento do modelo R1 pela DeepSeek, especialistas em IA suspeitaram que a "destilação" teria sido realizada pela DeepSeek. Finalmente, em 29 de janeiro, o Financial Times noticiou que a OpenAI confirmou ter visto "algumas evidências" de destilação, que "suspeitava serem da DeepSeek".<sup>52</sup>

Destilação, ou "destilação do conhecimento",<sup>53</sup> é uma técnica de aprendizado de máquina em que o conhecimento de um modelo grande e pré-treinado, o "professor", é transferido para um modelo menor e mais compacto, o "aluno". O objetivo é permitir que o modelo do aluno tenha o mesmo desempenho do professor, mas com recursos computacionais reduzidos ou limitados. Embora a técnica seja bem conhecida e comum, a OpenAI proíbe qualquer um de seus usuários de usar a destilação para construir um modelo rival, de acordo com seus termos de uso, como no uso de "saída para desenvolver modelos que competem com a OpenAI".<sup>54</sup>

De acordo com a Bloomberg,<sup>55</sup> pesquisadores de segurança da Microsoft observaram atividades de exfiltração de grandes quantidades de dados usando a interface de programação de aplicativos (API) da OpenAI, disponíveis apenas para usuários da OpenAI com licenças pagas, no outono do ano passado. A Microsoft, uma das principais parceiras e investidoras da OpenAI, notificou a empresa, informando

que as atividades eram suspeitas de serem originárias do DeepSeek.

Alguns usuários também relataram que os modelos de IA do DeepSeek frequentemente respondem a perguntas dizendo que são "IA desenvolvida pela Microsoft" ou "construída na arquitetura GPT-4 da OpenAI". A "rigidez e insistência" do modelo sobre "sua própria identidade como Microsoft Copilot" pode indicar o tipo de dados que os modelos do DeepSeek absorveram do OpenAI durante o treinamento.

Em 28 de janeiro, David Sacks, o czar da IA e das criptomoedas da Casa Branca, disse em uma entrevista à Fox que havia "evidências substanciais" de que a DeepSeek "destilou o conhecimento dos modelos da OpenAI".<sup>56</sup> Ele também disse que esperava que, nos próximos meses, as principais empresas de IA dos EUA tomassem medidas para "tentar impedir a destilação" para desacelerar "alguns desses modelos imitadores".

A OpenAI confirmou à Axios que reuniu "algumas evidências" de "destilação" de grupos sediados na China e está "ciente e analisando indícios de que a DeepSeek pode ter destilado indevidamente" modelos de IA.<sup>57</sup> A OpenAI trabalhará em estreita colaboração com o governo dos EUA para proteger sua tecnologia e seus "modelos mais capazes".

Será que tais alegações, se comprovadas, contradizem o que o fundador da DeepSeek, Liang Wenfeng, disse sobre sua missão de provar que as empresas chinesas podem inovar, em vez de apenas seguir? Nos últi-

52. [https://www.ft.com/content/a0dfedd1-5255-4fa9-8ccc-1fe01de87ea6?accessToken=zwAGLNJX-fBAkdOg3-3RUIVPqdOMzB\\_gHeh-pg.MEYCIQCGjo04z0mt0sKbDspQLq2BMXyw8SbQnlYePOuqiqr6QglhAlnK67eBkYuZS-77ljp-y--EJdN1wwRQ8GIR8sKMFgE&sharetype=gift&token=1eebbaa7-a4e6-4251-b665-c2f2562b38e4&mc\\_cid=486c7ce6ea](https://www.ft.com/content/a0dfedd1-5255-4fa9-8ccc-1fe01de87ea6?accessToken=zwAGLNJX-fBAkdOg3-3RUIVPqdOMzB_gHeh-pg.MEYCIQCGjo04z0mt0sKbDspQLq2BMXyw8SbQnlYePOuqiqr6QglhAlnK67eBkYuZS-77ljp-y--EJdN1wwRQ8GIR8sKMFgE&sharetype=gift&token=1eebbaa7-a4e6-4251-b665-c2f2562b38e4&mc_cid=486c7ce6ea)

53. <https://www.ibm.com/think/topics/knowledge-distillation>

54. <https://openai.com/policies/row-terms-of-use/>

55. <https://www.bloomberg.com/news/articles/2025-01-29/microsoft-probing-if-deepseek-linked-group-improperly-obtained-openai-data>

56. <https://www.foxnews.com/media/wake-up-call-us-leader-ai-says-white-house-ai-crypto-czar>

57. <https://www.axios.com/2025/01/29/openai-deepseek-ai-models-data-training>

mos dias, o governo chinês, especificamente o Departamento de Publicidade do Comitê Provincial de Zhejiang, também aderiu à DeepSeek e publicou um artigo elogiando a inovação, a confiança, a compostura e a confiança da empresa em seus jovens talentos.<sup>58</sup> A alegação de "destilação" muito provavelmente desencadeará um novo debate na comunidade chinesa sobre como os países ocidentais têm usado a proteção da propriedade intelectual como desculpa para suprimir o surgimento do poder tecnológico chinês.

A comunidade tecnológica chinesa pode contrastar a abordagem "altruísta" de código aberto da DeepSeek com os modelos ocidentais de IA, projetados apenas para "maximizar lucros e valores de ações". Afinal, a OpenAI está atolada em debates sobre o uso de materiais protegidos por direitos autorais para treinar seus modelos e enfrenta uma série de processos judiciais de autores<sup>59</sup> e organizações de notícias.<sup>60</sup> A OpenAI disse no ano passado que era "impossível treinar os principais modelos de IA de hoje sem usar materiais protegidos por direitos autorais".<sup>61</sup> O debate continuará.

Como os modelos de IA podem ser configurados e treinados com bastante facilidade, a segurança continua sendo crucial. Apesar dos recentes avanços das empresas chinesas de semicondutores no setor de hardware, os controles de exportação de chips avançados de IA e tecnologias de fabricação relacionadas têm se mostrado um impedimento eficaz.

Primeiro, os EUA ainda estão à frente em

## Por fim, que inferências podemos tirar do choque do DeepSeek?

IA, mas a China está logo atrás. David Sachs, o czar da IA e das criptomoedas dos EUA, reconheceu que as empresas chinesas estão "se recuperando muito rápido",<sup>62</sup> já que "o modelo DeepSeek-R1 é basicamente comparável em capacidades ao modelo OpenAI o1", que foi lançado há cerca de quatro meses. Ele posiciona os EUA em uma vantagem de apenas três a seis meses sobre os chineses.

Embora o DeepSeek tenha atraído muita atenção dos avanços recentes e futuros nos modelos de IA dos EUA nas últimas semanas, espera-se que o modelo o3 anunciado, mas ainda não lançado, da OpenAI implemente capacidades aprimoradas de resolução de problemas e raciocínio lógico aprimorado.<sup>63</sup> O episódio do DeepSeek pode muito bem se tornar um alarme e um lembrete muito necessários para a indústria de IA dos EUA investir para melhorar a proteção de sua propriedade intelectual e aplicar as regras do jogo relacionadas ao treinamento de dados para modelos.

Em segundo lugar, o gênio saiu da lâmpada. Os EUA ou qualquer empresa de IA não podem mais depender excessivamente do escalonamento por força bruta. Mesmo que seja possível provar que a DeepSeek se envolveu em destilação que violou os termos de uso da OpenAI, ainda há inúmeras inovações técnicas inegáveis e notáveis.<sup>64</sup> Desde recursos aprimorados de raciocínio em cadeia de pensamento (CoT) até a nova abordagem de apren-

58. <https://mp.weixin.qq.com/s/H0wizT8iwN406ERjdMLxLg>

59. <https://www.engadget.com/openai-and-microsoft-hit-with-copyright-lawsuit-from-non-fiction-authors-101505740.html>

60. <https://www.engadget.com/ai/the-new-york-times-says-openai-deleted-evidence-in-its-copyright-lawsuit-231805285.html>

61. <https://www.engadget.com/openai-admits-its-impossible-to-train-generative-ai-without-copyrighted-materials-103311496.html>

62. <https://www.foxnews.com/media/wake-up-call-us-leader-ai-says-white-house-ai-crypto-czar>

63. <https://www.analyticsvidhya.com/blog/2025/01/openai-o3-vs-competitors-performance-and-applications/>

64. <https://goodai.substack.com/p/beyond-the-hype-deepseeks-breakthroughs>

dizado por reforço (RL) adotada, a DeepSeek revelou diversas medidas de treinamento com boa relação custo-benefício.

Graças à DeepSeek, inovações semelhantes podem finalmente chamar a atenção de mais investidores do Vale do Silício. Marc Andreessen, investidor americano, postou no X que "DeepSeek R1 é o momento Sputnik da IA".<sup>65</sup> Tal percepção deve ser compartilhada por líderes governamentais, bem como por investidores e desenvolvedores. Se os EUA podem ver isso como seu "momento Sputnik", a China tem o mesmo direito e muito do que é necessário para aproveitar seu "momento Sputnik" também. A corrida para alcançar técnicas de raciocínio e otimização melhores e mais avançadas para treinamento em IA chegou com urgência crescente.

Terceiro, o governo e a indústria dos EUA devem perceber que a China tem um manual robusto para perturbar o ecossistema de IA liderado pelos EUA, e está mostrando sua força. Não só possui o conjunto de talentos para treinar e desenvolver modelos de IA extremamente competitivos e avançados internamente, como também consegue eliminar US\$1 trilhão do valor de mercado dos EUA em um dia,<sup>66</sup> incluindo cerca de US\$600 bilhões do valor da nVidia. O DeepSeek-R1 foi lançado "coincidentalmente" no mesmo dia da posse do presidente Trump. Para a intenção e o propósito da China, provavelmente não se trata apenas de perturbar a tecnologia e a indústria, mas também de perturbar o mercado e a economia de seu adversário.

Em quarto lugar, os EUA devem redobrar seus esforços no apoio à pesquisa fundamen-

tal e ao desenvolvimento de talentos. Ritwik Gupta, pesquisador de políticas de IA na Universidade da Califórnia, Berkeley, destacou que "a China tinha um grupo muito maior de engenheiros de sistemas do que os EUA, que entendiam como obter o melhor uso dos recursos computacionais e executar modelos de forma mais barata".<sup>67</sup>

Não se trata apenas de alcançar resultados com recursos limitados. Nos últimos anos, a China concentrou seus esforços de desenvolvimento de mão de obra em universidades nacionais e se beneficiou da permanência de mais talentos em tecnologia na China em vez de irem para o exterior, durante e após a COVID. Parte disso é consequência das políticas de educação e imigração dos EUA mais hostis em relação a estudantes e talentos estrangeiros. Em termos de apoio à pesquisa acadêmica e não comercial em IA, a Ordem Executiva de IA do governo Biden, que incluía apoio ao programa piloto para implementar o Recurso Nacional de Pesquisa em IA (NAIRR), foi revogada pelo governo Trump.

Além disso, a tentativa de Trump de congelar verbas federais abrangia "tudo, desde pesquisa em IA até fabricação de semicondutores", incluindo o NAIRR sob a National Science Foundation, bem como muitos projetos de pesquisa universitária. Até mesmo o investimento de US\$3,87 bilhões da empresa coreana de semicondutores SK Hynix em West Lafayette, Indiana,<sup>68</sup> foi suspenso devido ao congelamento do financiamento federal determinado pelo presidente, pois está vinculado a uma verba federal menor de US\$ 2,1 milhões para modernizar a in-

65. <https://x.com/pmarca/status/1883640142591853011>

66. <https://www.msn.com/en-us/money/other/deepseek-tech-wipeout-erases-more-than-1-trillion-in-market-cap-as-ai-panic-grips-wall-street/ar-AA1XXMT4>

67. <https://www.ft.com/content/747a7b11-dcba-4aa5-8d25-403f56216d7e>

68. <https://eng.sk.com/news/sk-hynix-signs-investment-agreement-of-advanced-chip-packaging-with-indiana>

fraestrutura municipal local e dar suporte à nova fábrica.<sup>69</sup> Felizmente, Trump revogou o congelamento após apenas um dia,<sup>70</sup> mas o risco constante de oscilação executiva — da imigração às tarifas e à assistência federal — continuará a gerar enormes incertezas quanto ao apoio do governo dos EUA à liderança tecnológica.

Quinto, a *DeepSeek também está afetando seus concorrentes chineses de IA e pode contribuir para reestruturar o futuro ecossistema de IA da China e do mundo*. O fato de uma pequena subsidiária de uma startup local de serviços financeiros ter conseguido tal avanço na engenharia deu ao governo, à indústria e à população do país um enorme impulso de confiança. Muitas outras iniciativas de apoio governamental ainda estão em andamento,<sup>71</sup> com coordenação de outros setores críticos, incluindo financiamento de bancos estatais.

O governo chinês parece encorajar essa competição acirrada em IA internamente. A DeepSeek já desencadeou uma guerra de preços entre modelos de IA na China no ano passado.<sup>72</sup> O Alibaba também acaba de lançar uma nova versão de seu modelo de IA e afirma que ele supera os desempenhos de referência da DeepSeek. Em outra nota, o analista de IA Alexander Doria relatou que, embora os modelos da DeepSeek tenham sido treinados em chips nVidia, eles se basearam nos chips Ascend 910C da Huawei de inferência para gerar respostas.<sup>73</sup> Se isso for verdade, os usuários do DeepSeek em todo o mundo, incluindo os americanos, podem estar gerando enormes demandas e utilização dos chips da Huawei, contribuindo para o ecossistema chinês de IA e semicondutores. Esta deveria

ser mais uma preocupação política para os formuladores de políticas dos EUA.

Finalmente, *os EUA precisarão desenvolver uma resposta à estratégia de código aberto da China em IA e outras áreas tecnológicas*. A DeepSeek e a China se orgulham da filosofia de código aberto<sup>74</sup> e, em parte porque não é nem mesmo uma startup de tecnologia, mas um "projeto paralelo" de um trader quantitativo, afirma que sua missão não é lucro. A empresa, até certo ponto, pegou o manto sem fins lucrativos exatamente onde a OpenAI o abandonou. A China contrastará sua "abertura" com os modelos proprietários dos EUA.

Esta é uma narrativa bem-vinda, adequada para uma nova iteração da estratégia da Rota da Seda Digital de IA da China, que deve ser música para os ouvidos de desenvolvedores e governos no Sul Global, ávidos por tecnologias de IA acessíveis que possam alavancar ao utilizar seus talentos locais para desenvolver setores de tecnologia domésticos e aplicações locais. O conceito de tecnologia de código aberto da China não se limita à IA; no entanto, ela permanece rigidamente controlada por seu governo, tornando suas plataformas e tecnologias de "código aberto" suscetíveis a vulnerabilidades e manipulação.

Se a estratégia dos EUA se concentrar apenas em apoiar o investimento em Big Techs, corre o risco de perder ainda mais o mercado mundial para a China. Uma repetição da incubação não intencional da Huawei se aproxima, só que potencialmente em uma escala ainda maior. Deve ter havido uma boa razão para a OpenAI ter começado como uma iniciativa sem fins lucrativos. Agora é um bom momento para visitar essa raiz. ■

69. <https://www.yahoo.com/news/projects-prep-chips-maker-sk-220801471.html>

70. <https://www.nytimes.com/live/2025/01/29/us/trump-federal-freeze-funding-news>

71. <https://foreignpolicy.com/2025/01/29/deepseek-china-ai-chatgpt-stocks/>

72. <https://finance.sina.com.cn/tech/2025-01-26/doc-inehksk9178057.shtml>

73. <https://x.com/Doriaalexander/status/1884167945280278857>

74. <https://mp.weixin.qq.com/s/H0wizT8iwN4O6ERjdMLxLg>

75. <https://jamestown.org/program/open-source-technology-and-prc-national-strategy-part-i/>

**Charles Mok** é pesquisador acadêmico na Incubadora de Políticas Digitais Globais do Centro de Políticas Cibernéticas da Universidade Stanford, membro do Conselho de Curadores da Sociedade da Internet e membro do conselho do Centro Internacional para Transparência e Monitoramento do Comércio. Charles atuou como membro eleito do Conselho Legislativo na Região Administrativa Especial de Hong Kong, representando o eleitorado funcional de Tecnologia da Informação, por dois mandatos, de 2012 a 2020. Em 2021, fundou a Tech for Good Asia, uma iniciativa para defender o uso positivo da tecnologia para empresas e comunidades civis. Como empreendedor, Charles foi cofundador da HKNet em 1994, um dos primeiros provedores de serviços de Internet em Hong Kong, que foi adquirido pela NTT Communications em 2000. Ele foi o presidente fundador da Sociedade da Internet de Hong Kong, presidente honorário e ex-presidente da Federação de Tecnologia da Informação de Hong Kong, ex-presidente da Associação de Provedores de Serviços de Internet de Hong Kong e ex-presidente da Organização Regional At-Large da Ásia, Austrália e Ilhas do Pacífico (APRALO) da ICANN. Charles é bacharel em Engenharia Elétrica e de Computação e mestre em Engenharia Elétrica pela Universidade Purdue.



# CMSI+20/WSIS+20

Uma pequena luz de esperança em um cenário político cada vez mais sombrio

Wolfgang Kleinwächter

Em 17 de dezembro de 2025 o presidente da 68ª Sessão Plenária da 80ª Assembleia Geral da ONU (AGNU)<sup>1</sup> aprovou por consenso a adoção do “Documento final da reunião de alto nível sobre a revisão geral da implementação dos resultados da Cúpula Mundial sobre a Sociedade da Informação +20”<sup>2</sup>. No entanto, os aplausos no grande salão do edifício da ONU, às margens do East River, foram contidos. Muitos governos se mostraram “igualmente insatisfeitos” com o texto final e deixaram claro que “consenso” não significa “acordo”.

## Um documento fraco ou um documento forte?

Os EUA rejeitaram todas as referências aos Objetivos de Desenvolvimento Sustentável (ODS)<sup>1</sup>, gênero e clima, e expressaram reservas sobre uma longa lista de parágrafos. O G77<sup>2</sup> e a China deixaram claro que, para eles, o pacote como um todo é muito fraco: não há compromissos financeiros claros para reduzir a exclusão digital, nem um papel reforçado para os governos na governança da Internet, nem menção ao princípio das responsabilida-

*Publicado originalmente em*

*<https://circleid.com/posts/wsis20-a-small-light-of-hope-in-a-darkening-political-landscape>*

des comuns, porém diferenciadas (RCPD)<sup>3</sup>.

A Rússia mostrou-se insatisfeita com o papel do Alto Comissariado das Nações Unidas para os Direitos Humanos, o Irã sentiu falta de um parágrafo importante sobre cooperação aprimorada, Israel se mostrou insatisfeito com as referências a problemas digitais em “territórios ocupados”, a Argentina discordou das referências à desinformação e ao discurso de ódio, a Ucrânia discordou do parágrafo que rejeita sanções unilaterais, a Arábia Saudita e a Nigéria se distanciaram das seções referentes à “violência sexual e de gênero” no parágrafo 11 e, para a Índia, o texto como um todo não foi considerado ambicioso o suficiente.

Por outro lado, o fato de, após seis meses de consultas com as partes interessadas e negociações intergovernamentais, ninguém ter se oposto à adoção do documento final, e ninguém ter solicitado uma votação, é motivo de celebração. A visão de 2005 de uma “sociedade da informação centrada nas pessoas, inclusiva e orientada para o desenvolvimento”, baseada no direito internacional e nos direitos humanos, foi reafirmada (parágrafo 1). O valor e os princípios da cooperação multissetorial foram reconhecidos como “vitais para o desenvolvimento da sociedade da informação” (parágrafo 2). E o Fórum de Governança da Internet (FGI/IGF)<sup>4</sup> passou a ser permanente (parágrafo 99). Tudo isso são boas notícias para os amigos da CMSI. A jornada da CMSI pode continuar. O documento final da CMSI+20 é o ponto de partida para a CMSI+30 em 2035.

Todos no Salão Plenário do edifício da ONU entenderam que aquele não era um momento histórico, nem um avanço que catapultasse a formulação de políticas digitais para um patamar superior. Era o nível mais básico, onde adversários podiam concordar,

independentemente das contradições que tivessem em outras áreas políticas. Mas a fragilidade do Documento Final da CMSI+20 é provavelmente a sua força. É sabido que vivemos tempos complexos.

Tendo em conta o contexto das tensões geopolíticas e estratégicas, foi uma decisão sábia dos dois cofacilitadores — os embaixadores da ONU da Albânia e do Quênia — não despertar questões já debatidas, trazendo para o centro das atenções da CMSI+20 os controversos problemas digitais da atualidade — cibercrime, ciberterrorismo, neocolonialismo digital, tributação digital, livre circulação transfronteiriça de dados confiáveis, uso indevido de redes sociais, vigilância em massa, bloqueios da Internet, censura online, domínio das empresas de tecnologia, sistemas de armas autônomas baseados na Internet, entre outros.

As ambições modestas preservaram a nobre visão do passado e deixaram a porta aberta para melhorias no futuro, quando o clima político permitir avanços maiores. A CMSI+20 provavelmente não foi um “sucesso extraordinário”, mas foi um sucesso, uma pequena luz de esperança em um cenário político sombrio. De uma perspectiva mais ampla, a CMSI+20 foi apenas um marco em um processo que começou no início do milênio e continuará no futuro. O fato de a corrente não ter se rompido na cidade de Nova York durante o rigoroso inverno político de 2025 é um resultado formidável.

## Velhas controvérsias em um novo ambiente

É interessante olhar para trás, para Genebra e Túnis. Ao final da primeira fase da CMSI (2003, em Genebra) houve um acordo sobre seus Princípios e Linhas

1. <https://sdgs.un.org/goals>

2. [https://pt.wikipedia.org/wiki/Grupo\\_dos\\_77](https://pt.wikipedia.org/wiki/Grupo_dos_77)

3. [https://en.wikipedia.org/wiki/Common\\_But\\_Differentiated\\_Responsibilities](https://en.wikipedia.org/wiki/Common_But_Differentiated_Responsibilities)

4. <https://www.intgovforum.org/>

de Ação, mas nenhum acordo sobre como financiar a exclusão digital e como governar a Internet.

No caminho para a segunda fase da CMSI (Túnis, 2005), dois órgãos subsidiários tentaram solucionar os problemas: uma Força-Tarefa sobre Mecanismo Financeiro (FTMF) abriu caminho para o estabelecimento de um Fundo Voluntário de Solidariedade Digital (FSD). Já o Grupo de Trabalho sobre Governança da Internet (GTGI) propôs a criação de um Fórum de Governança da Internet (FGI/IGF) como plataforma de discussão multissetorial, mas deixou em aberto a questão do papel que os governos deveriam desempenhar na governança da Internet.

Enquanto o FSD foi extinto em 2009 e a discussão sobre um órgão intergovernamental da Internet não produziu nada além de dois relatórios controversos do Grupo de Trabalho sobre Cooperação Aprimorada (GTCA) da Comissão sobre Ciência e Tecnologia para o Desenvolvimento (CCTD/UNCSTD), o FGI prosperou e criou um ecossistema único com uma ampla gama de atividades inter-sessãoais, órgãos subsidiários e mais de 170 FGIs nacionais e regionais.

Não foi exatamente uma surpresa que, nas negociações finais da CMSI+20, tenhamos tido um déjà vu: ninguém contestou a proposta de tornar o FGI permanente. Mas as outras duas questões — o mecanismo financeiro e o papel dos governos — voltaram à mesa de negociações. A diferença entre 2005 e 2025 foi que, há 20 anos, a Internet ainda era vista principalmente como uma questão técnica com algumas implicações políticas. Hoje, os problemas relacionados à Internet são questões políticas altamente sensíveis com um componente técnico. Isso tornou as antigas/novas controvérsias extremamente complexas.

## Do documento de elementos ao documento final de resultados

As negociações para o documento final começaram em junho de 2025 com a publicação de um “Documento de Elementos”, que foi amplamente debatido durante o FGI em Lilleström, Noruega, no fórum da CMSI em Genebra e em duas rodadas de consultas com as partes interessadas. As contribuições no debate permitiram que os cofacilitadores publicassem uma “Versão Zero” no final de agosto de 2025, que também foi discutida de forma aberta e transparente em uma série de consultas públicas, com mais de cem comentários por escrito das partes interessadas. Observações críticas foram incorporadas a uma versão revisada (Rev. 1), publicada em 7 de novembro de 2025. Essa versão também foi examinada criticamente por todas as partes interessadas, e as boas propostas serviram de base para uma segunda revisão (Rev. 2). A Rev. 2 constituiu a base para as negociações finais, que começaram em 9 de dezembro de 2025, na Sala 12, na sede da ONU.

Quando os governos se reuniram (participantes não estatais não foram autorizados a acompanhar as negociações finais), pareceu que a maioria estava bastante satisfeita com a linguagem de compromisso da Revisão 2. Mas, quando o grupo começou a analisar linha por linha as 20 páginas, a temperatura na sala 12 do subsolo da sede da ONU foi ficando cada vez mais fria. Na quinta-feira, 11 de dezembro, a maioria dos 127 parágrafos estava entre parênteses.

Para acomodar todas as críticas, os dois cofacilitadores elaboraram uma terceira revisão (Rev. 3) e a distribuíram aos Estados-membros sob o “procedimento de silêncio”, na esperança de alcançar consenso. Mas, quando o grupo de negociação se reuniu novamente na sexta-feira, 12 de dezembro, o

silêncio foi quebrado por alguns governos. Cinquenta e cinco dos 127 parágrafos da Rev. 3 foram contestados. E o governo dos EUA declarou que não estava em condições de apoiar o documento. Em outras palavras, todo o processo de revisão da CMSI+20 esteve à beira do colapso.

O que poderiam fazer os cofacilitadores em uma atmosfera tão congelada, onde cada um definia suas “linhas vermelhas”? Eles iniciaram consultas bilaterais com os mediadores do silêncio e ofereceram outra versão de compromisso durante o fim de semana (Rev.4), mas essa versão também encontrou oposição de diversos governos. Nesse momento, o presidente da 80ª Assembleia Geral da ONU interveio e, durante a noite, elaborou a versão final de compromisso, que foi apresentada na manhã de terça-feira, no início da reunião ministerial de alto nível.

Com esse texto, ninguém ficou realmente satisfeito. Mas, no fim das contas, a União Europeia, o Reino Unido, a Austrália, o Canadá, a Rússia, o Irã, a Arábia Saudita, o Iraque, Uganda, Cuba, o G77, a China e até mesmo os EUA reconheceram que é melhor ter um documento fraco e continuar o processo de 20 anos do que produzir outro desastre político.

## Mecanismo financeiro

Em relação ao financiamento, o consenso foi delegar a questão a um grupo de trabalho para elaborar propostas de ações futuras até 2027. No entanto, esse novo grupo de trabalho não será semelhante ao de 2004/2005. Desta vez, a União Internacional da Telecomunicação (UIT) foi convidada a criar um “Grupo de Trabalho interno para realizar uma avaliação das lacunas e desafios e apresentar recomendações concretas sobre o fortalecimento dos mecanismos financeiros para o desenvolvimento digital nos países em desenvolvimento” (parágrafo 67). Para o G77 e a

China, a criação de um grupo de trabalho para o financiamento da transformação digital era inegociável. Os EUA, a UE e o Reino Unido se opuseram à criação de uma nova instituição independente. Mas ambos os lados concordaram que é necessário mobilizar recursos para o desenvolvimento de infraestrutura, para a capacitação e para o investimento em inteligência artificial (IA).

Ter agora uma força-tarefa interna na UIT com o mandato de analisar as lacunas e os desafios é um compromisso razoável, mas é, na verdade, uma proposta muito frágil. Analisar as lacunas e os desafios para o desenvolvimento da infraestrutura de informação é o que a UIT faz desde a criação do seu setor UIT-D, há mais de 30 anos. A esperança é que a pressão da CMSI+20 impulsione a UIT para um novo patamar e que ela vá além da “Declaração de Baku”, adotada em novembro de 2025 na Conferência Mundial de Desenvolvimento das Telecomunicações (WTDC) da UIT, que declarou que “ninguém deve ficar para trás na era digital”.

A lição aprendida com o fracasso do FSD é que, em uma economia de mercado digital altamente competitiva, a expectativa de que esse fundo ajude a reduzir a exclusão digital é uma ideia ultrapassada. Foi interessante ouvir de muitos países em desenvolvimento que eles não esperavam dinheiro vivo dos países ricos. Eles reivindicavam parceria igualitária na economia digital e participação equitativa na formulação de políticas digitais globais. Reduzir a exclusão digital é, principalmente, um desafio de criar incentivos para o investimento privado em infraestrutura e aplicativos locais, bem como para parcerias público-privadas justas.

O ministro para assuntos digitais da Arábia Saudita, Abdullah Amer Alswaha, deixou claro que o país precisa, antes de tudo, de oportunidades de emprego, educação digital e inicia-

tivas locais no Sul Global. Se 90% dos mestrandos em IA forem formados em apenas um idioma, o resultado será desequilibrado. Isso precisa mudar.

## Governança da Internet

Uma observação semelhante pode ser feita em relação ao papel dos governos na governança da Internet. O plano de alguns governos após a Conferência de Túnis, de resolver os problemas no campo digital por meio da criação de um Conselho Intergovernamental da Internet, não funcionou nos últimos 20 anos. E não funcionará no futuro. No entanto, alguns governos do Sul Global, da Rússia e de outros países não estão satisfeitos com os mecanismos existentes, que deixam as “operações do dia a dia” na gestão de recursos críticos da Internet nas mãos de atores não governamentais. Eles queriam aproveitar a CMSI+20 para introduzir a ideia de “cooperação aprimorada” indiretamente no FGI, por meio da criação de uma “via governamental do FGI” com o mandato de negociar recomendações.

Recentemente, em setembro de 2024, o Pacto Digital Global (PDG)<sup>5</sup> reconheceu o FGI como a principal plataforma multissetorial para discussão de questões de governança da Internet. Uma via governamental independente dentro do FGI teria alterado a natureza multissetorial do fórum. Isso era inaceitável para os apoiadores do FGI.

A linguagem de compromisso no parágrafo 101 convida agora o FGI a “aprimorar suas modalidades de trabalho e ampliar a participação de governos e outras partes interessadas de países em desenvolvimento e comunidades sub-representadas, trabalhando para estabelecer e facilitar um diálogo entre governos com a participação de todas as partes interessadas”.

A linguagem parcialmente confusa do parágrafo 101 reflete as dificuldades que alguns governos têm em compreender a relação entre “multissetorialismo” e “multilateralismo”. Alguns governos desejam que a abordagem multissetorial esteja sob controle governamental. Outros consideram os governos como atores independentes dentro do modelo multissetorial.

Alguns governos pensam em termos de hierarquias, com o governo no topo. Outros entendem a sociedade moderna como uma rede, onde diferentes partes interessadas têm diferentes responsabilidades, mas trabalham em conjunto em pé de igualdade. É a visão de cima para baixo versus a de baixo para cima. O parágrafo 101 não resolve o problema, mas permite a continuidade do debate, mantendo a natureza multissetorial do FGI e convidando os governos a desempenharem um papel mais ativo.

## Multissetorialismo e multilateralismo

Este tema tem sido objeto de discussões controversas desde o primeiro FGI em Atenas, em 2006. Ao longo dos anos, consolidou-se o entendimento de que os dois conceitos não se excluem mutuamente, mas devem ser vistos como complementares. O sistema intergovernamental continua a desempenhar um papel importante, mas está inserido num ambiente multissetorial. O desenvolvimento de políticas digitais deve ser feito de baixo para cima e incluir todas as partes interessadas, incluindo os governos, conforme proposto pela definição de Governança da Internet da Agenda de Túnis.

A CMSI+20 reafirmou a definição de Túnis (parágrafo 88), que afirma que “a governança da Internet é o desenvolvimento e a aplicação, por governos, setor privado e sociedade civil,

5. <https://www.un.org/digital-emerging-technologies/global-digital-compact>

em seus respectivos papéis, de princípios, normas, regras, procedimentos de tomada de decisão e programas compartilhados que moldam a evolução e o uso da Internet”.

Uma das conquistas do processo CMSI+20 foi o fortalecimento da abordagem multissetorial, em comparação com a Agenda de Túnis de 2005 e o Documento Final da CMSI+10 de 2015. Nos 122 parágrafos da Agenda de Túnis, os termos “multissetorial” e “partes interessadas” apareceram 22 vezes. Nos 71 parágrafos da CMSI+10, os dois termos apareceram 19 vezes. Agora, temos 41 referências à abordagem multissetorial nos 127 parágrafos da CMSI+20.

Uma compreensão aprimorada desse conceito híbrido também se reflete no capítulo introdutório. O parágrafo 3 “reafirma o valor e os princípios da cooperação multissetorial”. O parágrafo 4 reafirma o “princípio da igualdade soberana de todos os Estados”. O documento começa com referências à abordagem multissetorial e continua com o papel dos governos. Em outras palavras, reconhece que o multilateralismo intergovernamental está inserido em um ambiente multissetorial. Multissetorialismo e multilateralismo são duas faces da mesma moeda. O que se faz necessário não é uma disputa entre as partes interessadas pela “liderança”, mas sim uma cooperação aprimorada entre todas as partes interessadas envolvidas, em seus respectivos papéis e em igualdade de condições.

É importante também que o Documento Final da CMSI+20 inclua, no parágrafo 94, uma referência às “Diretrizes Multissetoriais de São Paulo” da NetMundial, de abril de 2024<sup>6</sup>. Essas diretrizes foram além dos princípios acordados de governança da Internet e definiram com mais detalhes o “como” da cooperação multissetorial. Com essas dire-

trizes, a comunidade agora possui um critério para mensurar o nível real de multissetorialidade na formulação de políticas digitais. O fato de todos os 193 Estados-membros da ONU terem tomado conhecimento dessas diretrizes representa um pequeno, porém importante, passo rumo ao território ainda desconhecido do compartilhamento do desenvolvimento de políticas e da tomada de decisões entre as partes interessadas na era da ciberinterdependência.

Mas a realidade é que muitos governos apenas fingem apoiar o modelo multissetorial. Isso também se refletiu nas modalidades do processo preparatório da CMSI+20. Embora tenha havido um apoio formal ao modelo multissetorial, na prática, ele foi organizado em duas frentes de trabalho bastante separadas: consultas com atores não governamentais e negociações entre governos. Apenas um pequeno número de governos participou das consultas com atores não governamentais. E os atores não estatais foram excluídos das negociações intergovernamentais.

A ideia de estreitar os laços entre os dois grupos por meio da formação de um “Conselho Consultivo Multissetorial Informal” (CCMI) era boa. No entanto, seu sucesso foi limitado. O CCMI, que contou com o apoio integral dos dois cofacilitadores, tentou envolver os governos na discussão não governamental, ofereceu “horários de atendimento” para as partes interessadas e publicou declarações. Mas nem mesmo o CCMI teve permissão para permanecer como mero observador na sala de negociação.

Agora, após a CMSI+20, os governos têm a oportunidade, dentro de um FGI renovado, de demonstrar o seu interesse genuíno em compartilhar ideias e desenvolver políticas com outras partes interessadas. E a ideia inovado-

6. <https://netmundial.br/netmundial-10-multistakeholder-statement-strengthening-internet-governance-and-digital-policy-processes>

ra do CCMI como canal para organizar a comunicação entre as partes interessadas merece ser considerada em negociações futuras.

Por outro lado, o FGI, seu Grupo Consultivo Multissetorial (MAG) e seu Painel de Liderança também precisam fazer seus deveres de casa. Devem reconsiderar as modalidades do FGI e criar mais incentivos para o engajamento de todas as partes interessadas — governos, parlamentares, grandes e pequenas empresas, sociedade civil, comunidade técnica e acadêmica — a fim de criar um ambiente que comprove que o FGI é de fato “a principal plataforma multissetorial para discussão de questões de governança da Internet” e capaz de produzir resultados tangíveis que possam ser utilizados por todas as partes interessadas. O plano de estabelecer um novo “Grupo de Trabalho para o Aprimoramento do FGI” no âmbito do MAG é uma ideia que poderia ser útil para avançar nesse sentido.

Para cumprir esse papel, o FGI precisa de um orçamento estável e de um secretariado forte. O papel do secretariado do FGI em Genebra é reforçado no parágrafo 103, mas a questão do financiamento do FGI permanece sem solução. O documento final convida agora “o Secretário-Geral da ONU, com o apoio do Departamento de Assuntos Econômicos e Sociais das Nações Unidas (DAESNU/UNDESA), a apresentar uma proposta à Assembleia Geral durante a sua 80ª sessão para garantir o financiamento sustentável do Fórum”. O mandato da 80ª sessão da Assembleia Geral da ONU termina no início de setembro de 2026. Resta pouco tempo. Vamos aguardar para ver.

## **Direitos humanos, inteligência artificial, governança de dados e outras questões**

A lista de questões levantadas no documento final da CMSI+20 é extensa. Inclui também direitos humanos, economia digital,

desenvolvimento digital, cibersegurança, IA e governança de dados. No entanto, os capítulos sobre essas questões apenas reafirmam o que já havia sido decidido em outros contextos e fazem referência a outros processos.

Na seção sobre direitos humanos, há uma confirmação da resolução do Conselho de Direitos Humanos, que afirma que as pessoas devem desfrutar dos mesmos direitos tanto offline quanto online. Os parágrafos relacionados à liberdade de expressão, à proteção da privacidade e à vigilância em massa repetem a linguagem do documento da CMSI+10 e do PDG. A novidade reside na formulação clara do papel do Alto Comissariado das Nações Unidas para os Direitos Humanos. Este é um passo importante para garantir que a CMSI esteja fundamentada nos direitos humanos.

O PDG também é visto como a estrutura adequada para a discussão sobre IA e governança de dados. No âmbito do PDG, dois novos órgãos da ONU para IA foram recentemente criados: o Painel Científico Internacional sobre IA e o Diálogo Global sobre Governança de IA. Esse primeiro diálogo global ocorrerá em Genebra, em julho de 2026, juntamente com o fórum da CMSI. O PDG também recomendou a criação de um Grupo de Trabalho sobre Governança Digital (GTGD), que já iniciou seus trabalhos na primavera de 2025 e deve apresentar seu relatório final à CCTD, em Genebra, até 2027.

A seção sobre a economia digital apela a um “ambiente aberto, justo e não discriminatório para o desenvolvimento digital” (parágrafo 30) e convida a “combater as concentrações de capacidade tecnológica e poder de mercado, a fim de garantir que os benefícios da cooperação digital sejam distribuídos de forma justa” (parágrafo 31). Trata-se de uma linguagem bastante polida que evita abordar questões controversas como a tributação digital, discutida no Grupo de Negociações Internacionais

(GNI) da Convenção das Nações Unidas sobre Tributação, ou o Pacto de Comércio Digital, conforme debatido na OMC.

A seção de cibersegurança saúda o estabelecimento do novo “Mecanismo Global” sobre cibersegurança no âmbito da 1ª Comissão da Assembleia Geral da ONU, como seguimento do “Grupo de Trabalho Aberto”, mas não faz qualquer menção à Convenção das Nações Unidas contra o Cibercrime (Convenção de Hanói), que está aberta para assinatura desde outubro de 2025. Ignora também as discussões no âmbito da Convenção sobre Armas Convencionais sobre sistemas de armas autônomas baseados na Internet e o uso de IA no domínio militar.

Será necessário ter mãos habilidosas para coordenar todas essas atividades no futuro. A CMSI+20 exige coerência e evita duplicação. De uma forma ou de outra, todos os novos processos de formulação de políticas digitais têm suas raízes na CMSI e se baseiam no uso da internet. A definição de governança da Internet da Agenda de Túnis é ampla e também relevante para a governança cibernética, a governança digital, a governança da Internet das Coisas, a governança de dados ou a governança da IA. Não há necessidade de reinventar a roda.

Na medida em que é positiva, a CMSI está agora intimamente ligada à revisão do PDG, agendada para 2027, e à revisão dos ODS, agendada para 2030. É também positivo que o papel do Grupo das Nações Unidas para a Sociedade da Informação seja reforçado e que o este tenha recebido um mandato para promover o diálogo multissetorial (parágrafo 121).

Isso permite uma análise mais abrangente de todos os novos processos emergentes. A arquitetura da CMSI continua a crescer. Ela agora engloba as Linhas de Ação da CMSI, os ODS da ONU, o PDG, o FGI, o Fórum da CMSI com sede em Genebra, o Diálogo Global

sobre Inteligência Artificial, o Painel Científico Internacional sobre Inteligência Artificial e o GTGD da CCTD.

Uma coordenação bem-sucedida exige uma relação estreita entre as diversas instituições e escritórios da ONU. ECOSOC, ETDE e DAESNU, em Nova York, precisam trabalhar em conjunto com o Secretariado do FGI, o CCTD e o GNUSI, em Genebra. Na sociedade da informação, tudo está interligado. O Painel de Alto Nível da ONU sobre Cooperação Digital estava certo quando afirmou, já em 2019: “Vivemos na era da ciberinterdependência”.

## Governo dos EUA

Um novo problema no contexto da CMSI foi o papel do governo dos EUA. Por mais de 20 anos, o governo dos EUA foi um parceiro construtivo no desenvolvimento da abordagem multissetorial para a formulação de políticas digitais. Mas, após a reunião da CCTD em abril de 2025, em Genebra, onde o governo dos EUA votou contra a resolução da CMSI+20, que preparou o terreno para as negociações de revisão da CMSI+20 em Nova York, permaneceu incerta até o último momento qual seria a posição do governo dos EUA.

Após a apresentação da Rev.3, o governo dos EUA indicou que provavelmente convocaria uma votação sobre o documento final da CMSI+20. Foi nesse momento que um grupo de importantes organizações de tecnologia dos EUA se mobilizou e escreveu uma carta ao Departamento de Estado americano, solicitando a continuidade do apoio dos EUA ao FGI e à abordagem multissetorial.

Quando a reunião de alto nível começou na manhã de terça-feira com declarações de governos e representantes não governamentais, os EUA se abstiveram de tomar a palavra. Não houve declaração dos EUA na tarde de terça-feira. Nem na manhã de quarta-feira. Somente na sessão da tarde de quarta-fei-

ra, os EUA tomaram a palavra como o último orador e declararam que não pediram uma votação, apesar de suas reservas em relação a muitas partes do texto final. Em uma “Explicação de Posição” antes da votação, o governo dos EUA se distanciou de vários parágrafos do documento, mas declarou que continuará a apoiar a abordagem multissetorial.

## E agora?

A CMSI+20 foi um teste de resistência para os governos, demonstrando que, apesar das profundas controvérsias, os mecanismos multilaterais ainda estão ativos e podem produzir resultados. Mas, provavelmente, o mais importante foi o efeito mobilizador que a CMSI+20 teve sobre as partes interessadas não governamentais.

A Coalizão Global pelos Direitos Digitais organizou a sociedade civil, a Coalizão da Comunidade Técnica para o Multissetorialismo uniu a comunidade técnica e a Câmara de Comércio Internacional reuniu pequenas e grandes empresas em apoio aos principais valores da CMSI, como a abordagem multissetorial para a governança da Internet. Os diversos grupos de partes interessadas não governamentais publicaram documentos de posicionamento e declarações com propostas concretas sobre como aprimorar a cooperação multissetorial, conforme o “Plano de Cinco Pontos para uma CMSI+20 Inclusiva”. O estabelecimento do CCMI foi outra inovação.

Essas atividades mostraram ao mundo que os princípios da CMSI, como abertura, transparência, responsabilidade, inclusão, desenvolvimento participativo de políticas e compartilhamento de normas, regras, princípios, programas e tomada de decisões, não são uma visão abstrata, mas fazem parte da realidade da comunidade da Internet.

Manter esse engajamento coordenado será fundamental para a implementação dos compromissos da CMSI+20. Um FGI renovado e aprimorado em 2026, as próximas reuniões do GTGD da CCTD, o Diálogo Global sobre Governança de IA em Genebra, em julho de 2026, o início do novo Mecanismo Global de Segurança Cibernética em Nova York, em março de 2026, a Conferência de Plenipotenciários da UIT no Catar, em novembro de 2026, e outros eventos já estão preenchendo a agenda para o ano. E em 2027, a revisão da Convenção sobre Diálogo Global (PDG) está logo ali.

Ellie McDonald e Lea Kaspar, da Global Partners Digital, uma ONG que coordenou o engajamento da sociedade civil no processo da CMSI+20, resumiram o resultado final da maneira correta:

“O resultado da CMSI+20 deve ser entendido como um ponto de transição, e não como um encerramento. À medida que a implementação começa, a prestação de contas será um teste crucial da credibilidade da estrutura. Os compromissos assumidos no texto final — incluindo os relativos a direitos humanos, abordagens multissetoriais e o combate às persistentes desigualdades digitais — exigirão acompanhamento constante. Uma tarefa fundamental para a comunidade em geral será monitorar a implementação e responsabilizar os governos pelos compromissos assumidos. O fato de a CMSI funcionar como uma estrutura viva para a cooperação digital ou se tornar meramente formal dependerá menos da linguagem acordada do que de como esses compromissos serão colocados em prática no período subsequente.” ■

**Wolfgang Kleinwächter** é Professor Emérito de Políticas e Regulação da Comunicação Internacional no Departamento de Estudos de Mídia e Informação da Universidade de Aarhus, na Dinamarca. Ele está envolvido com questões de governança da Internet desde o início da década de 1990. Participou ativamente da Cúpula Mundial da Sociedade da Informação (CMSI) da ONU, onde foi membro do Grupo de Trabalho da ONU sobre Governança da Internet (GTGI), do Fórum de Governança da Internet (FGI), onde foi Conselheiro Especial da Presidência de 2006 a 2011, e da ICANN, onde presidiu, entre outras funções, o Comitê de Nomeações (NomCom) e é membro do Conselho da GNSO desde 2011. É cofundador do Diálogo Europeu sobre Governança da Internet (EURODIG) e membro do Grupo de Trabalho de Aprimoramento do FGI da UNCSTD. É também fundador e presidente da “Escola de Verão Europeia sobre Governança da Internet” (EURO-SSIG). Já publicou e editou mais de 200 artigos e 12 livros.

## Apêndice: Siglas no texto

<b>Sigla PT-BR</b>	<b>Sigla EN</b>	<b>Descrição</b>
AGNU	UNGA	Assembleia Geral das Nações Unidas
CCMI	IMSB	Conselho Consultivo Multissetorial Informal
CCTD	UNCSTD	Comissão sobre Ciência e Tecnologia para o Desenvolvimento
CMDT	WTDC	Conferência Mundial de Desenvolvimento da Telecomunicação
CMSI	WSIS	Cúpula Mundial da Sociedade da Informação
DAESNU	UNDESA	Depto. de Assuntos Econômicos e Sociais das Nações Unidas
ECOSOC	ECOSOC	Conselho Econômico e Social das Nações Unidas
ETDE	ODET	Escritório para Tecnologias Digitais e Emergentes
FGI	IGF	Fórum de Governança da Internet
FSD	DSF	Fundo de Solidariedade Digital
FTMF	TFFM	Força-Tarefa sobre Mecanismo Financeiro
GCM	MAG	Grupo Consultivo Multissetorial [do IGF]
GNUSI	UNGIS	Grupo das Nações Unidas para a Sociedade da Informação
GTCA	WGEC	Grupo de Trabalho sobre Cooperação Aprimorada
GTGD	DGWG	Grupo de Trabalho sobre Governança Digital
IA	AI	Inteligência Artificial
ODS	SDG	Objetivos de Desenvolvimento Sustentável
OMC	WTO	Organização Mundial do Comércio
PDG	GDC	Pacto Digital Global
RCPD	CBDR	Responsabilidades Comuns Porém Diferenciadas
UIT	ITU	União Internacional da Telecomunicação





# POLITICS

[ <https://politics.org.br> ]

A revista **POLITICS** é uma publicação do Nupef . ISSN: 1984-8803 [ [nupef.org.br](http://nupef.org.br) ] [ [politics.org.br](http://politics.org.br) ]

[ publicado em julho de 2025 ]





# POLITICS

[ politics.org.br ]



O Nupef é uma organização sem fins de lucro, dedicada à reflexão, análise, produção de conhecimento e formação, principalmente centradas em questões relacionadas às Tecnologias da Informação e Comunicação (TICs) e suas relações políticas com os direitos humanos, a democracia, o desenvolvimento sustentável e a justiça social.

Além de realizar cursos, eventos, desenvolver pesquisas e estudos de caso, o Nupef edita a POLITICS, a Rets (Revista do Terceiro Setor) e mantém o projeto Tiwa – um centro de serviços Internet que serve de apoio técnico aos projetos do instituto e das entidades parceiras. Para saber mais acesse [nupef.org.br](http://nupef.org.br).



O Núcleo de Informação e Coordenação do Ponto BR - NIC.br foi criado para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br, que é o responsável por coordenar e integrar as iniciativas e serviços da Internet no País.

O NIC.br, além de braço executivo do CGI.br, tem entre suas atribuições: o registro e manutenção dos nomes de domínios que usam o .br; o tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil; projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País. Para saber mais acesse [nic.br](http://nic.br).