



Pontifícia
Universidade
Católica do
Rio de Janeiro

Estella Regueira Thompson

**VIGILÂNCIA COMO PODER:
Recomendações para coleta e uso de dados à sociedade
civil rumo a uma nova ética digital**

Trabalho de conclusão de curso

Trabalho de Conclusão de Curso apresentado ao Instituto de Relações Internacionais da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) como requisito parcial para obtenção do título de bacharel em Relações Internacionais.

Orientador: Prof. Guilherme Ferreira Sorgine

Rio de Janeiro
Dezembro de 2025

Todos os direitos reservados. É proibida a reprodução total ou parcial do trabalho sem autorização da universidade, do/a autor/a e do orientador.

Estella Regueira Thompson

Estudante do curso de Graduação em Relações Internacionais do IRI / PUC-Rio.

Ficha Catalográfica

Regueira Thompson, Estella

Vigilância como poder: recomendações para coleta e uso de dados à sociedade civil rumo a uma nova ética digital / Estella ; orientador: Guilherme Ferreira Sorgine. – 2025.

45 f.; 30 cm

Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2025.

Inclui bibliografia.

1. Relações internacionais – Trabalhos de conclusão de curso. 2. Capitalismo de vigilância. 3. Sociedade civil. 4. Governança digital. 5. Inteligência artificial. 6. Coleta de dados. I. Jesus, Diego Santos Vieira de. II. Pontifícia Universidade Católica do Rio de Janeiro. Instituto de Relações Internacionais. III. Título.

CDD: 327

Agradecimentos

A conclusão deste trabalho representa muito mais do que o fim de um ciclo acadêmico; ela simboliza o percurso de amadurecimento que vivi ao longo da minha graduação. Nenhuma parte desta trajetória seria possível sem as pessoas que me cercaram, me sustentaram e me inspiraram.

Agradeço, antes de tudo, à minha família, base de tudo o que sou e de tudo o que construo. À minha mãe e à minha avó, Sofia e Lana, que sempre foram referências de força, sensibilidade e perseverança. Elas acompanharam cada etapa deste processo, ofereceram apoio incondicional nos momentos de incerteza e celebraram comigo cada conquista. O exemplo que carrego em suas histórias e atitudes orientou minhas escolhas e me guiou ao longo de toda a graduação.

À PUC-Rio e ao Instituto de Relações Internacionais, minha sincera gratidão por terem se tornado espaços de descoberta, reflexão e acolhimento. Sou profundamente grata aos professores que contribuíram para minha formação, ampliaram meu olhar sobre o mundo e me incentivaram a buscar rigor, ética e profundidade intelectual. Cada aula, conversa e desafio acadêmico deixaram marcas que levarei comigo para toda a vida.

Agradeço especialmente ao meu orientador, professor Guilherme, pela orientação atenta, pelo compromisso acadêmico e por acreditar no potencial deste trabalho desde as primeiras conversas. Sua dedicação e disponibilidade foram fundamentais para que este projeto ganhasse forma. Ao professor Diego, segundo avaliador deste trabalho e professor querido, agradeço pelo olhar crítico, pelas sugestões precisas e pela generosidade em contribuir para o amadurecimento desta pesquisa e especialmente pelo cuidado e carinho desde o meu primeiro dia de graduação.

Quero também registrar meu reconhecimento às amizades que construí ao longo destes anos. Foram laços que cresceram em meio a salas de aula, trabalhos e na empresa júnior. Essas pessoas se tornaram parte essencial da minha jornada, oferecendo leveza nos períodos mais intensos e compartilhando entusiasmo nas descobertas que fizemos juntos. O apoio, a parceria e a sinceridade dessas amizades transformaram minha experiência universitária em algo muito maior do que formação acadêmica.

Por fim, agradeço ao meu namorado, Gabriel, por ser presença constante e afetuosa em todos os momentos. Seu apoio emocional, sua paciência e sua capacidade de me tranquilizar nas horas de maior pressão foram fundamentais para que eu concluísse esta etapa com equilíbrio e confiança. Sua parceria torna meus caminhos mais leves e meus objetivos mais possíveis.

Ao meu companheiro de curso, Rafael, vai um agradecimento especial. Obrigada por dividir comigo o último e mais intenso ano de graduação e por ter me acompanhado na jornada de desenvolvimento do trabalho secundário de conclusão de curso no eixo de comércio, nada disto seria possível sem a nossa parceria.

A todos que contribuíram, com palavras, gestos, ensinamentos ou companhia, para que este trabalho se realizasse, deixo minha gratidão mais sincera. Este trabalho carrega um pouco de cada um que caminhou comigo.

Resumo

Regueira Thompson, Estella; Sorgine, Guilherme Ferreira (Orientador).
Vigilância como poder: recomendações para a coleta e o uso de dados à sociedade civil rumo a uma nova ética digital Rio de Janeiro, 2025, 45 p.
Trabalho de Conclusão de Curso de Graduação – Instituto de Relações Internacionais, Pontifícia Universidade Católica do Rio de Janeiro.

A pesquisa busca, a partir da exposição de como o capitalismo de vigilância, intensificado pelo avanço da Inteligência Artificial, transformou a coleta e o uso de dados pessoais em um mecanismo estrutural de poder, e oferecer recomendações a governos, universidades, escolas, veículos de mídia e organizações sociais a fim de contribuir para a formação de consciência crítica na sociedade civil acerca da coleta e do uso de dados pessoais, em ambientes virtuais, num contexto conducente a novas formas de governança que valorizem a ética e os direitos fundamentais no mundo digital.

Palavras-chave

Capitalismo de vigilância; Sociedade civil; Governança digital; Inteligência artificial; Coleta de dados

Abstract

Regueira Thompson, Estella; Sorgine, Guilherme Ferreira (Advisor). **Surveillance as power:** recommendations for data collection and use directed at civil society toward a new digital ethics. Rio de Janeiro, 2025. 45 p. Undergraduate Final Paper – International Relations Institute, Pontifical Catholic University of Rio de Janeiro.

The research seeks to examine how surveillance capitalismo, intensified by advances in Artificial Intelligence, has transformed the collection and use of personal data into a structural mechanism of power, and to offer recommendations for governments, universities, schools, media outlets, and civil society organizations aimed at fostering critical awareness among citizens regarding the collection and use of personal data in virtual environments. The study is situated within a context that calls for new forms of governance that prioritize ethics and the protection of fundamental rights in the digital world.

Keywords

Surveillance capitalism; Civil society; Digital governance; Artificial intelligence; Data collection

Sumário

Principais resultados	10
1. Introdução	11
1.1. Problema	
1.2. Objeto da pesquisa	12
1.3. Metodologia da pesquisa	13
1.4. Objetivo central e alinhamento com os Objetivos de Desenvolvimento Sustentável	14
2. Engrenagem de poder	15
2.1. Da revolução digital ao capitalismo de vigilância	
2.2. Estados Unidos e China: disputa pela regulação de plataformas	17
3. Dados, poder e rivalidade geopolítica	19
3.1. Regulação como instrumento de poder	
3.2. Papel da IA e do controle de dados na intensificação da rivalidade	21
3.3. Consequências globais da disputa	23
4. Estudos de caso	26
4.1. Tiktok: dados, narrativas e segurança da informação	
4.2. Chat GPT: IA generativa e novos dilemas regulatórios	30
5. Conclusão	34
6. Caminhos de cooperação e recomendações	35

Lista de Figuras

Figura 1 - A engenharia das recomendações

Lista de Boxes

Box 1 - Capitalismo de vigilância

Lista de quadros

Quadro 1 - Méritos e limitações do avanço das plataformas digitais

Principais resultados

- O capitalismo de vigilância se consolidou como um modelo global de poder, transformando dados pessoais em um recurso estratégico explorado por grandes plataformas digitais.
- Avanços da Inteligência Artificial ampliaram a escala e a opacidade da coleta de dados, reforçando assimetrias informacionais entre empresas, Estados e cidadãos.
- A sociedade civil permanece estruturalmente vulnerável, com baixa compreensão sobre como seus dados são utilizados para moldar comportamentos e fluxos de informação, mesmo sendo um dos agentes da engrenagem.
- A governança digital internacional apresenta forte fragmentação, agravada pela disputa geopolítica entre Estados Unidos e China.
- Iniciativas de educação digital crítica e participação cidadã ainda são insuficientes para equilibrar o poder informacional concentrado nas plataformas.
- As recomendações propõem caminhos concretos, como padrões internacionais, auditorias independentes, interoperabilidade regulatória e fortalecimento da participação social, para ampliar transparência, ética e proteção de direitos no ambiente digital.

1. Introdução

1.1. Problema

A partir da análise do capitalismo de vigilância e do avanço da IA, emerge um dilema central da era digital: como garantir transparência, veracidade soberania informacional e proteção de direitos fundamentais em um contexto em que o poder político e econômico se concentra nas mãos de grandes plataformas e corporações tecnológicas. A coleta massiva e contínua de dados transformou a experiência digital cotidiana em fonte de lucro e controle, e nesse cenário, o problema não se limita à ausência de um marco regulatório internacional capaz de equilibrar inovação e proteção de dados, mas também à falta de consciência sobre a profundidade e as implicações desse modelo econômico.

Empresas como TikTok e OpenAI ilustram essa nova configuração, em que a regulação de plataformas deixou de ser um tema meramente técnico para se tornar um instrumento de influência, especialmente entre Estados Unidos e China, enquanto a disputa entre essas potências molda os rumos da governança global da tecnologia, a sociedade, principal produtora de dados, permanece alheia às dinâmicas que determinam como suas informações são coletadas, processadas e utilizadas. Essa assimetria informacional reforça a passividade social nas decisões que definem os rumos do espaço digital.

O problema da pesquisa, portanto, reside na ausência de mecanismos efetivos de governança e, sobretudo, de consciência pública sobre o capitalismo de vigilância e o uso massivo de dados pessoais, que transformaram a sociedade em um ator inconsciente dentro da disputa geopolítica por informação e poder. Diante disso, a questão orientadora que guia esta pesquisa é: como o capitalismo de vigilância e a regulação das plataformas digitais, impulsionados pelo avanço da Inteligência Artificial, consolidam um sistema global de poder baseado na exploração de dados, evidenciado pela disputa entre os Estados Unidos e China já citados e de que forma a falta de informação e conscientização da sociedade civil,

agente na estrutura do capitalismo de vigilância, contribui para a perpetuação dessa assimetria deixando-a alheia ao que acontece por trás dos panos?

1.2. Objeto de pesquisa

Ao longo da pesquisa, pretendo analisar, sob a ótica da exclusão da sociedade civil, como o avanço acelerado das IA se insere nesse contexto, consolidando o domínio das grandes corporações tecnológicas cuja vantagem competitiva repousa sobre o acesso privilegiado a bancos de dados globais. Essa concentração de informação cria assimetrias de poder, não somente entre empresas e usuários, mas entre Estados, sobretudo na disputa geopolítica entre Estados Unidos e China, que transformou a regulação de plataformas digitais em um campo estratégico de afirmação de soberania e influência internacional. Casos como ChatGPT e TikTok e ChatGPT exemplificam de forma clara como a tecnologia passou a ser tratada como questão de segurança nacional e instrumento de poder normativo, capaz de moldar padrões éticos, políticos e culturais em escala mundial.

Aqui, o objeto de pesquisa é a interrelação entre plataformas digitais, Inteligência Artificial, capitalismo de vigilância e cooperação internacional para o desenvolvimento no contexto da governança global, com ênfase em como essas transformações impactam diretamente a vida cotidiana dos cidadãos e a percepção coletiva e empresarial sobre privacidade, autonomia e poder.

A leitura da obra de Shoshana Zuboff, que introduziu o conceito de capitalismo de vigilância para descrever o modo como dados pessoais passaram a ser extraídos, processados e comercializados como o principal recurso econômico da era digital, revelou a dimensão estrutural desse fenômeno, em que a coleta massiva de dados redefine as relações entre Estado, mercado e indivíduo, assim como sua face invisível e socialmente naturalizada: a participação cotidiana de bilhões de usuários em um sistema que opera com pouca transparência e sem plena consciência de seus mecanismos.

1.3. Metodologia da pesquisa

A pesquisa adota uma abordagem qualitativa, de caráter descritivo e analítico, fundamentada em uma perspectiva crítica das relações entre tecnologia, poder e sociedade. Seu propósito é compreender como o capitalismo de vigilância, sustentado pela coleta e uso massivo de dados, afeta as estruturas democráticas e a autonomia individual. A metodologia foi escolhida para aproximar o debate teórico da realidade social, buscando traduzir fenômenos da economia digital em elementos acessíveis e socialmente relevantes.

O estudo baseia-se em revisão bibliográfica e documental, abrangendo obras clássicas e contemporâneas sobre capitalismo de vigilância, governança digital, inteligência artificial e regulação de plataformas. Autores como Shoshana Zuboff, Manuel Castells, Byung-Chul Han e Evgeny Morozov servem de referência central para a análise crítica da lógica de vigilância e de sua dimensão política. Além disso, serão examinados relatórios e documentos oficiais de organizações multilaterais, como ONU, OCDE e UNESCO, que abordam os desafios éticos e regulatórios das tecnologias digitais.

A metodologia também inclui a análise de casos emblemáticos, como TikTok e ChatGPT, que ilustram de que forma as plataformas digitais se tornaram arenas de disputa entre grandes potências, ao mesmo tempo em que afetam diretamente os usuários comuns. Esses estudos de caso servirão como ponto de partida para discutir as implicações sociais da concentração de dados e a ausência de consciência pública sobre sua circulação e utilização.

Por fim, a pesquisa se propõe a articular esse diagnóstico teórico e empírico com uma reflexão, com o objetivo de produzir uma análise acadêmica, mas também um instrumento de conscientização, capaz de evidenciar os riscos e responsabilidades associados à vida digital contemporânea. Busca-se, assim, contribuir para a construção de uma cidadania digital crítica, que reconheça o valor político dos dados e reivindique maior transparência, equidade e responsabilidade no uso das tecnologias de informação e comunicação.

1.4. Objetivo central e alinhamento com os Objetivos de Desenvolvimento Sustentável

Mais do que propor um modelo institucional de governança internacional, este trabalho pretende contribuir para a formação de uma consciência crítica na sociedade civil. O intuito é demonstrar que a comercialização e o controle de dados, hoje concentrados nas mãos de um número restrito de corporações e Estados, especialmente Estados Unidos e China, não constituem só uma disputa geopolítica abstrata, mas um processo que redefine as fronteiras da privacidade, da cidadania e da própria democracia.

O trabalho tem, portanto, um duplo propósito: de um lado, esclarecer como a dinâmica global de dados reflete e reproduz hierarquias geopolíticas e econômicas; de outro, fomentar a conscientização sobre os riscos de uma participação passiva nesse sistema, apontando recomendações e caminhos possíveis para uma cultura digital mais informada e responsável, em que cidadãos compreendam o valor de seus dados, reconheçam as assimetrias envolvidas em sua exploração e desenvolvam práticas individuais e coletivas de proteção, resistência e exigência de transparência.

2. Engrenagem de poder

2.1. Da revolução digital ao capitalismo de vigilância

Há cerca de 200 mil anos a espécie dos *Homo Sapiens* surge na África Oriental. Apenas 130 mil anos mais tarde, ocorre a revolução cognitiva, o surgimento da linguagem ficcional e os *sapiens* começam a se espalhar pelo mundo, povoando a Austrália, seguida da América. Deste momento em diante, as grandes transformações da humanidade demoraram milhares de anos para acontecer. A revolução agrícola surgiu há 12 mil anos; cerca de 5 mil anos atrás nasceram os primeiros reinos, a escrita, o dinheiro e as religiões organizadas; há 500 anos tivemos a revolução científica e, há 200 anos, a revolução industrial.

Hoje, no entanto, as evoluções parecem acontecer do dia para a noite. A revolução digital, iniciada há aproximadamente 5 décadas, já transformou completamente a forma como nos comunicamos e trabalhamos. Agora, assistimos a uma aceleração ainda mais intensa: um salto tecnológico que, em questão de meses, redefine indústrias inteiras, desafia conceitos éticos e nos obriga a repensar o que significa ser humano em um mundo moldado por máquinas inteligentes.

No mundo moderno, as plataformas digitais passaram a fazer parte das rotinas, classificadas como redes orquestradas por um controlador, essas ferramentas hoje ditam nossos hábitos, mediando desde o consumo de informações até a forma como nos relacionamos social e economicamente. Mais do que simples canais de interação, elas se tornaram verdadeiras infraestruturas digitais, responsáveis por organizar fluxos de trabalho, lazer e consumo, condicionando comportamentos de maneira quase invisível. Nesse contexto, a coleta e análise em larga escala de dados tornaram-se o alicerce de seus modelos de negócio, permitindo um nível de personalização e de monitoramento sem precedentes.

Quadro 1 – Méritos e limitações do avanço das plataformas digitais

MÉRITOS	LIMITAÇÕES
Integram-se ao cotidiano e facilitam rotinas.	Ditam hábitos e condicionam comportamentos de maneira invisível.
Funcionam como infraestruturas digitais que organizam trabalho, lazer e consumo.	Centralizam fluxos sociais, econômicos e informacionais sob controle de um único operador.
Permitem personalização de serviços por meio da análise de dados.	Baseiam-se em coleta massiva de dados, criando modelos de vigilância permanentes.
Mediando interações, ampliam acesso à informação e conexões sociais.	Transformam-se em mecanismos de monitoramento contínuo, reduzindo autonomia e previsibilidade sobre como dados são usados.

Fonte: Zuboff, 2019

Nesse contexto, a coleta e análise em larga escala de dados tornaram-se o alicerce de seus modelos de negócio, permitindo um nível de personalização e de monitoramento sem precedentes. A obra da acadêmica americana Shoshana Zuboff, apresenta o modelo onde os comportamentos individuais são monitorados e convertidos em “excedente comportamental”, utilizado para prever e até influenciar ações futuras.

Box 1 - Capitalismo de vigilância

O conceito de capitalismo de vigilância, é entendido como um novo regime econômico que transforma a experiência humana em matéria-prima gratuita para práticas de extração, previsão e comercialização de dados.

Fonte: Zuboff, 2019.

Mais do que um sistema de negócios, Zuboff mostra que o capitalismo de vigilância representa uma nova forma de poder, capaz de moldar decisões, condutas e relações sociais, consolidando mecanismos de controle sem precedentes na história.

Supletivamente, o nascimento das Inteligências Artificiais, que nada mais são do que máquinas, alimentadas por dados, capazes de raciocinar, aprender e atuar de maneira que normalmente exigiria inteligência humana, marca uma virada decisiva no desenvolvimento tecnológico. Diferente de outras inovações, a IA aprende com cada interação, expandindo continuamente sua capacidade de previsão e tomada de decisão. Essa característica a torna especialmente poderosa em uma conjuntura em que os dados são o novo recurso estratégico mais valioso. Contudo, junto às oportunidades, surgem os dilemas éticos e sociais, como a concentração de poder nas mãos de poucos controladores de dados, um fator que redefine relações de poder e pode determinar os rumos da sociedade.

2.2. Estados Unidos e China: a disputa pela regulação de plataformas

Em uma corrida, é natural que aquele que parte antes disponha de maiores condições de alcançar a linha de chegada em vantagem. No campo da tecnologia, a lógica não se altera: o pioneirismo, somado ao investimento contínuo e à capacidade de transformar descobertas em sistemas de larga escala, tende a consolidar a liderança de determinadas nações. O domínio tecnológico, nesse sentido, resulta de um processo histórico de acumulação e de estratégias deliberadas de inovação.

A rivalidade entre Estados Unidos e China adquire relevância particular no cenário contemporâneo da economia digital. Os Estados Unidos consolidaram sua primazia tecnológica ao longo do século XX, ancorados em uma tradição de inovação que culminou no ecossistema do Vale do Silício e na emergência de conglomerados privados que moldaram a infraestrutura global da internet.

A China, por sua vez, intensificou sua presença a partir do início do século XXI, amparada por uma estratégia estatal orientada para o desenvolvimento tecnológico, que promoveu a ascensão de gigantes corporativos nacionais e assegurou autonomia em setores estratégicos.

Nas últimas décadas, essa trajetória convergente resultou na concentração, por parte de ambos os países, das principais infraestruturas de dados e dos investimentos em Inteligência Artificial. A disputa, que já não se limita à esfera econômica, tornou-se um elemento estruturante da geopolítica contemporânea.

Ao longo da história, as grandes potências foram responsáveis por inaugurar ou acelerar transformações que alteraram o curso da humanidade. Estados Unidos e China ocupam hoje esse papel central. A posição de liderança que exercem decorre tanto de trajetórias históricas de inovação quanto da ampla disponibilidade de recursos financeiros, tecnológicos e humanos, em escala que excede a dos países em desenvolvimento. Tal assimetria reforça a condição dessas duas nações como protagonistas de um modelo emergente de poder, sustentado pelo controle de dados e pela capacidade de utilizá-los como fundamento de novas formas de organização.

3. Dados, poder e rivalidade geopolítica

3.1 Da revolução digital ao capitalismo de vigilância

Ao longo da história, o poder internacional esteve profundamente associado ao domínio sobre os recursos estratégicos de cada época. No século XVII e XVIII, durante o auge do mercantilismo, o acúmulo de ouro e prata simbolizava a força das nações e determinava seu prestígio no sistema internacional. Nos séculos seguintes, com o avanço da industrialização e o fortalecimento do capitalismo moderno, o controle sobre matérias-primas, energia e tecnologia industrial passou a definir a hierarquia entre os Estados. No século XX, especialmente após as guerras mundiais, o poder se expressava pela capacidade de produzir e distribuir petróleo, sustentar um aparato militar robusto e projetar influência cultural e diplomática, em outras palavras, a combinação entre *hard power* e *soft power*.

No século XXI, esse eixo de poder migra para um novo campo: o domínio da informação e dos dados. Em uma economia digitalizada, o mundo gera atualmente cerca de 400 milhões de terabytes de dados por dia, o que equivale a mais de 147 zettabytes por ano, consolidando os dados como o principal recurso estratégico do século XXI.

A informação deixou de ser apenas um insumo para a tomada de decisões e passou a constituir o próprio fundamento do poder político, econômico e social.

Nesse contexto, essa regulação das plataformas digitais emerge como um elemento central da geopolítica contemporânea. O que antes era uma discussão restrita ao campo jurídico ou tecnológico, envolvendo privacidade e segurança cibernética, passou a ter implicações diretas sobre a distribuição de poder global, sem a participação da principal peça para o funcionamento da engrenagem: a sociedade. Cerca de 65 % da infraestrutura mundial de armazenamento e processamento de dados está sob jurisdição norte-americana, enquanto a China

responde por aproximadamente 20 %, refletindo uma nova forma de concentração e dependência digital (Synergy Research Group, 2024; Telegeography, 2024).

As normas que definem como os dados são coletados, processados e transferidos entre fronteiras configuram novas formas de dependência e influência entre os Estados. A disputa pela regulação digital tornou-se, portanto, uma disputa pela própria soberania no mundo interconectado enquanto a esfera civil é excluída do debate.

Os Estados Unidos e a China representam polos opostos nessa arena. O modelo norte-americano privilegia a inovação e a autorregulação das empresas privadas, partindo da crença de que o livre mercado estimula o avanço tecnológico e o crescimento econômico. Em 2024, os Estados Unidos investiram cerca de US\$109 bilhões em inteligência artificial, enquanto a China destinou US\$9,3 bilhões, revelando prioridades distintas em inovação e controle. Já o modelo chinês adota uma abordagem estatal e centralizada: o governo exerce controle direto sobre as plataformas e sobre o fluxo de dados, integrando-as ao aparato de segurança nacional, conforme previsto na Data Security Law (2021). Essa dicotomia revela duas visões distintas de poder digital, uma baseada na liberdade corporativa e outra ancorada na soberania estatal. No entanto, ambas convergem na percepção de que controlar os dados é essencial para projetar poder e garantir influência internacional.

Plataformas digitais ilustram como empresas tecnológicas se tornaram agentes geopolíticos. Elas medeiam comunicações e transações enquanto hoje moldam percepções, definem padrões de comportamento e influenciam processos políticos. O TikTok, com cerca de 1,6 bilhão de usuários ativos mensais, coleta padrões de digitação, localização, histórico de navegação e metadados de vídeos, o que gerou investigações e tentativas de banimento nos Estados Unidos sob alegações de risco à segurança nacional. Esse caso exemplifica como decisões regulatórias podem ser usadas como instrumentos de contenção estratégica. A tensão sobressai o campo econômico e assume caráter ideológico, confrontando visões distintas sobre privacidade, liberdade e controle informacional do meio social.

Dessa forma, a regulação das plataformas digitais transcende o debate técnico e passa a refletir poder no sistema internacional. Relatórios da OCDE (2024) e da ONU (Resolução A/RES/78/265, 2024) indicam que a ausência de

padrões comuns em governança digital amplia as desigualdades informacionais e cria novas hierarquias tecnológicas. Quem define as regras sobre dados, algoritmos e inteligência artificial define também os limites do possível no campo político e econômico. O controle sobre os fluxos informacionais é, hoje, um dos meios mais sutis e eficazes de exercer influência global. Nesse sentido, compreender a regulação digital é compreender as novas dinâmicas da rivalidade entre potências, uma disputa travada não em campos de batalha, mas nas redes, nos servidores e nos códigos que estruturam a vida contemporânea.

3.2 O papel da IA e do controle de dados na intensificação da rivalidade

A consolidação da IA como tecnologia estratégica ampliou a dimensão da disputa digital. A tecnologia depende de grandes volumes de dados para aprender, prever e automatizar decisões, e, portanto, reforça a centralidade do acesso informacional como ativo geopolítico. Em 2025, o volume global de dados criados e processados está com projeção de alcançar 181 zettabytes, demonstrando a escala crescente da matéria-prima informacional que sustenta os sistemas de IA.

Países e empresas que dominam a infraestrutura de coleta e processamento de dados passam a deter uma vantagem estrutural na corrida tecnológica e militar. Cerca de 65% da infraestrutura mundial de data centers está concentrada em território norte-americano, enquanto 20% encontra-se sob jurisdição chinesa, o que traduz o novo mapa da interdependência digital (Synergy Research Group, 2024; Telegeography, 2024). Nesse contexto, o controle dos fluxos digitais deixa de ser apenas uma questão econômica e se transforma em tema de segurança nacional.

Nos Estados Unidos, o desenvolvimento da IA está concentrado em conglomerados privados como Google, Microsoft e OpenAI, que operam sob lógica de mercado e inovação contínua. A OpenAI, por exemplo, registra mais de 700 milhões de usuários semanais e processa bilhões de tokens de texto diariamente, segundo seu relatório oficial de 2024, enquanto empresas como

Microsoft e Google Cloud detêm quase 66% do mercado global de nuvem, infraestrutura essencial para o treinamento de modelos de linguagem.

Já na China, empresas como Baidu e Alibaba atuam em sintonia com as diretrizes estatais, integrando seus sistemas ao projeto nacional de liderança tecnológica e vigilância populacional, conforme previsto no Plano “Next Generation Artificial Intelligence Development” (State Council, 2017) e reforçado pela Data Security Law (2021). O resultado é uma intensificação das rivalidades entre as potências, em termos econômicos e normativos: trata-se de uma disputa sobre como e para que a tecnologia deve ser usada.

Assim, a regulação da IA torna-se o novo campo de batalha internacional. Cada país busca moldar padrões éticos, técnicos e jurídicos que reflitam seus interesses. A União Europeia aprovou em 2024 o *AI Act (Regulation 2024/1689)*, o primeiro marco legal abrangente sobre IA no mundo, estruturado em um modelo de regulação por níveis de risco e baseado em princípios de transparência, rastreabilidade e supervisão humana (European Parliament, 2024).

Em paralelo, a ONU aprovou a Resolução A/RES/78/265 (2024), que defende o uso “seguro, confiável e alinhado aos direitos humanos” da IA, sinalizando um esforço multilateral de harmonização (United Nations, 2024). Já os Princípios de IA da OCDE (2019, atualizados em 2024) reforçam os eixos de *accountability, fairness e human-centered design*, sendo adotados por mais de 50 países (OECD.AI Observatory, 2024). [ET2] Conclui-se, portanto, que apesar de estarem sendo construídos mecanismos para impor limites ao instrumento de vigilância, tais mecanismos permanecem mantendo os cidadãos à margem.

Enquanto isso, os Estados Unidos e a China exportam suas arquiteturas tecnológicas e normativas para países emergentes: Washington aposta em padrões de mercado abertos e cooperação público-privada (NIST AI Risk Management Framework, 2023), enquanto Pequim promove acordos bilaterais de infraestrutura digital e uso de IA sob supervisão estatal, especialmente no Sudeste Asiático e na África (NIST, 2023; MIIT China Digital Economy Report, 2024). Assim, a corrida tecnológica se converte em uma corrida regulatória, na qual estabelecer padrões significa definir quem exercerá a autoridade moral e técnica sobre a Inteligência.

3.3 Consequências globais da disputa

A fragmentação da governança digital produz efeitos que ultrapassam o campo tecnológico. O primeiro deles é a erosão da privacidade individual, uma vez que cidadãos em todo o mundo passam a ter seus dados coletados, analisados e comercializados sem plena consciência ou consentimento. Dos dados que o mundo gera hoje, mais de 90% são processados por empresas privadas com fins comerciais, segundo a OCDE (Digital Economy Outlook, 2024). A ausência de padrões internacionais uniformes gera assimetrias profundas: apenas 71 países possuem leis de proteção de dados abrangentes, enquanto mais de 100 ainda carecem de qualquer marco regulatório efetivo, de acordo com o Banco Mundial (World Development Report, 2023). Em regiões de baixa renda, menos de 30% da população possui garantias legais contra vigilância digital, o que evidencia o abismo normativo entre o Norte e o Sul Global (ITU, *Facts and Figures 2024*).

Enquanto alguns países protegem rigidamente os direitos de seus usuários, como a União Europeia, sob o Regulamento Geral de Proteção de Dados (GDPR), outros exploram a coleta de dados como ferramenta de vigilância ou de vantagem competitiva. Estudo da UNESCO (2023) indica que mais de 70% das nações que adotaram tecnologias de reconhecimento facial não estabeleceram mecanismos de consentimento explícito, o que amplia o risco de abusos e monitoramento político.

No plano econômico, a disputa afeta o comércio internacional e as cadeias globais de valor. Relatórios da UNCTAD (Digital Economy Report, 2023) mostram que o fluxo internacional de dados movimenta hoje o equivalente a US\$ 11 trilhões anuais, superando o valor do comércio físico de bens manufaturados. Entretanto, políticas de *data localization* e restrições à transferência transfronteiriça de informações aumentaram mais de 300% desde 2017, tornando-se instrumentos de política industrial e de proteção econômica (UNCTAD, 2023; OECD, 2024). Como consequência, empresas que dependem de dados globais enfrentam custos médios 40% maiores para operar em múltiplas jurisdições, segundo o World Economic Forum (2024). Assim, o controle dos fluxos digitais redefine os centros de inovação e investimento, concentrando benefícios em países com infraestrutura robusta de nuvem e regulação flexível.

Além disso, o campo da segurança cibernética é profundamente impactado. Em 2024, foram registrados mais de 2,3 bilhões de incidentes de ciberataques no mundo, um aumento de 26% em relação ao ano anterior, de acordo com o Global Threat Report (CrowdStrike, 2025). Práticas como espionagem digital, manipulação de informações e guerras híbridas tornaram-se formas correntes de competição entre Estados. A ONU (Resolução A/RES/79/239, 2024) reconhece formalmente o uso da inteligência artificial em contextos militares como uma das principais ameaças emergentes à paz internacional, evidenciando a sobreposição entre poder tecnológico e segurança global, o que para a sociedade representa cada vez mais exposição a riscos invisíveis e contínuos, nos quais seus dados, sua segurança e até sua percepção da realidade podem ser manipulados por atores poderosos sem que ela sequer perceba.

Desse modo, vemos que há implicações diretas para a democracia. A manipulação algorítmica, a desinformação e o uso político das plataformas desafiam a transparência e a confiança nas instituições. Relatório do Pew Research Center (2024) indica que 64% dos usuários de internet acreditam que as redes sociais têm impacto negativo sobre a democracia, e mais de 70% relatam ter sido expostos a conteúdo enganoso online no último ano. Esses dados mostram que a rivalidade digital não se limita à disputa por poder material, mas incide sobre os fundamentos da convivência social e dos regimes democráticos. A Resolução da Assembleia Geral da ONU sobre “Integridade da Informação no Espaço Digital” (A/RES/78/311, 2024) destaca a urgência de combater a desinformação e proteger direitos humanos no ambiente online, recomendando cooperação multilateral para restaurar a confiança pública.

A nova ordem informacional é, simultaneamente, um espaço de inovação e de conflito, exigindo novas formas de governança e cooperação internacional que possam equilibrar soberania, liberdade e responsabilidade coletiva, guiando um caminho para o desenvolvimento. A OCDE (Digital Economy Outlook, 2024) e a UNESCO (Ethics of AI Report, 2023) enfatizam o desafio: garantir que a revolução digital sirva ao interesse público e não à concentração de poder

4. Estudos de caso

4.1 Tiktok: dados, narrativas e segurança da informação

O caso do TikTok tornou-se um dos exemplos mais emblemáticos de como a regulação de plataformas pode se transformar em instrumento geopolítico. O aplicativo, desenvolvido pela empresa chinesa ByteDance, ultrapassou a marca de 1 bilhão de usuários ativos em todo o mundo e mais de 170 milhões apenas nos Estados Unidos, tornando-se uma das redes sociais de maior alcance global. No entanto, essa expansão acentuou as tensões entre Estados Unidos e China, pois a plataforma passou a ser vista tanto como um produto de entretenimento, quanto como um vetor de coleta massiva de dados e, assim, um potencial instrumento de influência estrangeira. Essa percepção transformou o TikTok em um verdadeiro campo de batalha regulatória, onde segurança da informação, soberania digital e competição estratégica se entrelaçam.

Em 2024, o Congresso norte-americano aprovou o Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA), legislação que determinava que a ByteDance deveria vender o controle do TikTok a uma empresa americana sob pena de banimento da plataforma no país. A justificativa oficial foi a proteção da segurança nacional, sustentada pelo argumento de que o governo chinês poderia exigir acesso aos dados dos usuários norte-americanos. Em janeiro de 2025, o presidente Donald Trump assinou uma ordem executiva adiando a entrada em vigor da lei por 75 dias, após forte mobilização pública e pressão de influenciadores e criadores de conteúdo que dependem economicamente da plataforma (People, 2025). A decisão, no entanto, não encerrou a disputa: o caso chegou à Suprema Corte, que manteve a constitucionalidade da lei, reafirmando que o risco à segurança nacional justificava a intervenção (Reuters, 2025).

A narrativa predominante nos Estados Unidos associa o TikTok à possibilidade de espionagem digital e manipulação informacional. Relatórios da Center for Strategic and International Studies (CSIS) apontam que o aplicativo

coleta uma gama extremamente ampla de informações, incluindo localização, histórico de navegação, interações, dados biométricos, padrões de digitação e até o nível de bateria dos dispositivos, o que lhe confere uma capacidade de monitoramento superior à de qualquer outra plataforma popular (CSIS, 2023). Além disso, o modelo de negócios da rede social baseia-se em um algoritmo de recomendação altamente sofisticado, cuja eficácia depende justamente da amplitude e da granularidade dos dados coletados. O resultado é um ciclo retroalimentado: quanto mais o usuário interage, mais a plataforma compreende seus hábitos, preferências e vulnerabilidades, o que potencializa sua capacidade de moldar comportamentos e capturar atenção, característica central do capitalismo de vigilância, conceito desenvolvido por Shoshana Zuboff (2019).

A combinação entre coleta massiva de dados e mecanismos de influência algorítmica tem implicações diretas tanto para a segurança nacional quanto para a autonomia individual. Esse tipo de arquitetura digital reforça assimetrias de poder entre usuários e plataformas, na medida em que os primeiros desconhecem o alcance real do monitoramento a que estão sujeitos. A própria empresa admite utilizar dados de navegação e localização para aprimorar a personalização de conteúdo e direcionar publicidade, o que amplia o potencial de exploração econômica e de manipulação política desses dados.

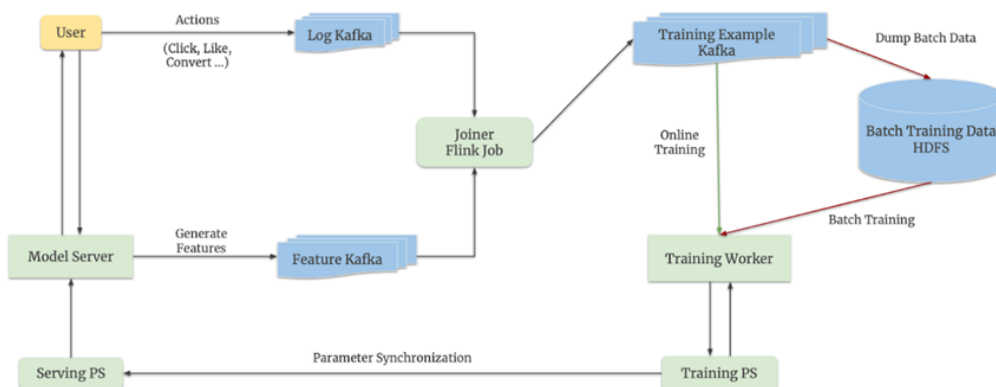
Do ponto de vista da segurança da informação, especialistas alertam para o risco de que a concentração de dados sob controle de uma empresa sediada em um regime autoritário crie vulnerabilidades para os Estados ocidentais. O governo chinês mantém leis de cibersegurança que obrigam empresas nacionais a cooperar com autoridades em caso de interesse estatal. Assim, mesmo que a ByteDance negue qualquer compartilhamento indevido de dados, a possibilidade jurídica de acesso governamental já é suficiente para acender o alerta sobre riscos potenciais (CSIS, 2023; The Verge, 2024). Nos Estados Unidos, essa percepção resultou em ações coordenadas: além da pressão política, diversas agências federais e governos estaduais proibiram o uso do aplicativo em dispositivos oficiais, reforçando o discurso de proteção à segurança nacional.

Entretanto, a discussão em torno do TikTok transcende a dimensão da espionagem e atinge o campo da liberdade de expressão e da governança global da informação. A empresa argumenta que o banimento constitui uma forma de censura digital e uma violação da Primeira Emenda da Constituição

norte-americana, que garante o direito à livre manifestação. Essa tensão revela um dilema contemporâneo: como equilibrar a necessidade de regulação e proteção de dados com a preservação de direitos fundamentais. Ao mesmo tempo, evidencia a instrumentalização política da regulação tecnológica, utilizada como ferramenta de contenção econômica e simbólica de rivais geopolíticos.

O caso também ilustra a assimetria de poder que caracteriza o atual sistema internacional da informação. Enquanto os Estados Unidos e a China disputam a definição das normas e dos padrões tecnológicos globais, a sociedade civil, permanece à margem desse processo, muitas vezes sem plena consciência de como seus dados são coletados, armazenados e monetizados. Essa falta de transparência e de educação digital amplia a vulnerabilidade dos cidadãos e reforça a urgência de um debate público sobre privacidade, ética tecnológica e soberania digital. Nesse sentido, o caso TikTok serve como exemplo de disputa geopolítica e como alerta sobre a fragilidade dos mecanismos de proteção à informação em escala global.

Além dos riscos à privacidade e à soberania, há impactos sociais e psicológicos que decorrem do modelo algorítmico do TikTok. De acordo com relatório da Amnesty International (2023), o sistema de recomendação da plataforma pode expor usuários, especialmente crianças e adolescentes, a conteúdos prejudiciais, reproduzindo vieses e reforçando padrões de consumo e comportamento potencialmente nocivos. Isso demonstra como os algoritmos, alimentados por dados pessoais, não apenas organizam o fluxo informacional, mas moldam o imaginário coletivo e influenciam a formação de opinião. Assim, o poder do TikTok ultrapassa o campo econômico e alcança a esfera simbólica, configurando uma nova forma de dominação baseada na atenção e na predição comportamental. A arquitetura do sistema de recomendações do aplicativo ilustra de forma concreta como o capitalismo de vigilância opera silenciosamente através da coleta contínua, integração e processamento de dados pessoais. O diagrama abaixo, retirado do artigo técnico *Monolith: The Recommendation System Behind TikTok*, revela o funcionamento interno do mecanismo que atualiza modelos preditivos em tempo real a partir das interações dos usuários, cliques, curtidas, tempo de visualização e padrões de engajamento.

Figura 1 – A engenharia das recomendações

Fonte: Gantry, 2023

Esse sistema funciona em um ciclo permanente de retroalimentação: cada ação do usuário é registrada (via *Log Kafka*), convertida em atributos comportamentais (*features*) e imediatamente utilizada para ajustar o modelo de recomendação por meio de *online training*. A atualização contínua dos parâmetros, especialmente das camadas esparsas de *embeddings*, que representam preferências individuais altamente granulares, permite ao TikTok reagir quase instantaneamente a mudanças de interesse. Na prática, isso significa que o aplicativo aprende o que o usuário “quer” e adapta o conteúdo em questão de minutos.

Esse mecanismo evidencia como a plataforma captura microvariações comportamentais para maximizar engajamento, reforçando a centralidade dos dados como recurso estratégico. O usuário, ao interagir de maneira aparentemente banal, alimenta um sistema sofisticado que transforma cada gesto em informação comercializável. Trata-se de um exemplo emblemático do capitalismo de vigilância: a extração contínua de dados comportamentais produz *insights* que são convertidos em poder preditivo e, consequentemente, em vantagem econômica e geopolítica.

Além disso, há impactos sociais e psicológicos decorrentes desse modelo. Segundo a Amnesty International (2023), o sistema de recomendação do TikTok tende a expor usuários, sobretudo crianças e adolescentes, a conteúdos potencialmente prejudiciais, reforçando vieses, padrões de consumo e até

tendências autodestrutivas. As recomendações não se limitam a organizar o fluxo de informações: elas moldam percepções, influenciam comportamentos e constroem visões de mundo de forma altamente personalizada e opaca. Assim, o poder do TikTok ultrapassa a esfera econômica e alcança a dimensão simbólica, configurando um tipo de dominação baseada na atenção e na predição comportamental.

Ao analisar seu funcionamento interno, torna-se evidente que o TikTok não é apenas um aplicativo de entretenimento, mas um dispositivo de captação e modelagem comportamental em escala global. Seu sistema de recomendações representa um caso exemplar de como dados individuais são convertidos em *soft power* digital, integrando lógicas econômicas, tecnológicas e geopolíticas que sustentam a disputa contemporânea entre grandes potências pelo controle da infraestrutura informacional do século XXI.

Do ponto de vista do seu enquadramento teórico, o estudo de caso do TikTok coaduna com o argumento central deste trabalho: a regulação de plataformas digitais não é um processo neutro ou puramente técnico, mas um espaço de disputa entre interesses econômicos, políticos e estratégicos. A forma como Estados e empresas lidam com a coleta e o controle de dados reflete as lógicas de poder do sistema internacional. Ao mesmo tempo, evidencia a necessidade de conscientização da sociedade civil sobre as implicações desse modelo, afinal, o que está em jogo não é apenas a segurança de informações individuais, mas a própria estrutura de poder que define quem controla o conhecimento, a comunicação e o futuro digital.

4.2 Chat GPT: IA generativa e novos dilemas regulatórios

O caso do ChatGPT, desenvolvido pela OpenAI, representa um marco na discussão global sobre Inteligência Artificial e regulação de plataformas. Lançado em novembro de 2022, o modelo rapidamente atingiu mais de 100 milhões de usuários em apenas dois meses, tornando-se o aplicativo de crescimento mais rápido da história segundo a UBS Evidence Lab (2023). Sua popularização evidenciou tanto o potencial transformador da IA generativa quanto as lacunas

normativas que envolvem privacidade, transparência algorítmica e uso ético de dados. O ChatGPT passou a simbolizar o novo estágio do capitalismo de vigilância: o da extração, processamento e recombinação massiva de informações textuais, visuais e comportamentais para alimentar sistemas capazes de gerar conteúdo, raciocinar e interagir com humanos de forma autônoma.

O funcionamento desses modelos depende da coleta de grandes volumes de dados públicos e privados, utilizados para treinar redes neurais de larga escala. Relatórios do Stanford Institute for Human-Centered Artificial Intelligence (2024) indicam que modelos como o ChatGPT foram treinados com trilhões de palavras, extraídas de bases de dados públicas, publicações científicas, redes sociais e conteúdos gerados por usuários. Esse processo revela a dimensão material dos dados como novo recurso econômico global, comparável ao petróleo durante o século XX, mas com implicações políticas mais complexas: quem controla o fluxo e a qualidade dos dados controla também a capacidade de desenvolver tecnologias de ponta e de definir padrões de governança digital.

Desde 2023, diferentes governos e organismos internacionais têm buscado lidar com esses desafios. A União Europeia aprovou o AI Act (2024), o primeiro marco legal abrangente sobre Inteligência Artificial no mundo, estabelecendo categorias de risco e impondo obrigações de transparência e segurança a sistemas generativos como o ChatGPT. Nos Estados Unidos, o governo lançou a AI Executive Order (Casa Branca, 2023), que estabelece diretrizes sobre segurança, direitos civis e inovação responsável, embora ainda privilegie a autorregulação corporativa. A China, por sua vez, publicou as Medidas Provisórias para Serviços de IA Generativa (2023), que impõem controle estatal direto sobre os modelos e o conteúdo gerado, reforçando a dimensão de soberania digital que caracteriza sua política tecnológica. Essas diferentes respostas ilustram a diversidade de paradigmas regulatórios que coexistem no sistema internacional, tema central do seu trabalho.

Em 2023, o ChatGPT foi temporariamente suspenso na Itália, após o órgão regulador de proteção de dados, o Garante per la Protezione dei Dati Personali, apontar possíveis violações ao Regulamento Geral de Proteção de Dados (GDPR). As preocupações incluíam a coleta de informações de menores sem consentimento

e a ausência de base legal clara para o tratamento de dados pessoais usados no treinamento do modelo (BBC News, 2023). O episódio gerou repercussões globais e levou a OpenAI a adotar medidas de transparência, como permitir que usuários solicitem exclusão de seus dados e que países exijam relatórios sobre conformidade regulatória. Esses acontecimentos revelam a tensão entre inovação acelerada e proteção de direitos, problema recorrente nas discussões sobre capitalismo digital e governança internacional.

O poder de influência da IA generativa vai além do campo técnico. Modelos como o ChatGPT reconfiguram a forma como o conhecimento é produzido, distribuído e consumido. A automatização da linguagem e a personalização das respostas consolidam novas formas de intermediação informacional, nas quais empresas privadas definem, de maneira opaca, o que é relevante ou verdadeiro. Essa assimetria informacional cria riscos à privacidade e também à pluralidade de ideias e à autonomia intelectual. De acordo com o Center for AI and Digital Policy (2024), os sistemas generativos têm o potencial de amplificar vieses, difundir desinformação e reforçar estruturas de poder já existentes, reproduzindo desigualdades cognitivas e culturais em escala global.

Além das questões de segurança e ética, há implicações geopolíticas diretas. O desenvolvimento de modelos de IA de larga escala requer infraestrutura computacional avançada, acesso privilegiado a chips de alto desempenho e disponibilidade massiva de dados, recursos concentrados majoritariamente em empresas dos Estados Unidos e da China. Essa concentração reforça a dependência tecnológica de outros países e amplia o fosso digital, criando uma nova hierarquia global baseada no controle de dados e da capacidade de processamento. Como observam analistas do Brookings Institution (2024), a IA generativa tornou-se o novo eixo da rivalidade estratégica entre Washington e Pequim, substituindo parcialmente a corrida por hardware e semicondutores pela disputa por inteligência algorítmica e padrões normativos.

Essa disputa se manifesta também no campo da governança. Enquanto os Estados Unidos defendem uma abordagem flexível, centrada na inovação e na liderança corporativa, a China busca projetar um modelo de controle estatal e nacionalismo tecnológico. No meio desse embate, a sociedade civil global

enfrenta um déficit de informação e de capacidade crítica para compreender os impactos dessa transformação. Usuários comuns interagem diariamente com ferramentas baseadas em IA sem plena consciência de que seus dados, preferências e padrões de comportamento estão sendo utilizados para alimentar sistemas que aprendem, preveem e moldam suas interações futuras. Esse é o ponto de interseção entre o caso do ChatGPT e o problema central deste trabalho: a urgência de ampliar a conscientização pública sobre o papel dos dados na nova economia digital e sobre os riscos da concentração de poder informacional em poucas mãos.

A ascensão do ChatGPT demonstra que o poder no século XXI se traduz cada vez mais na capacidade de processar e interpretar dados. As plataformas que detêm esse controle passam a influenciar decisões políticas, econômicas e culturais, redefinindo a própria noção de soberania. A ausência de uma governança global coerente para regular o uso da Inteligência Artificial aprofunda a fragmentação digital e aumenta a vulnerabilidade dos cidadãos e dos Estados menos desenvolvidos. A questão que se impõe é como equilibrar inovação e responsabilidade, liberdade e segurança, avanço tecnológico e proteção de direitos fundamentais.

Dessa forma, o caso do ChatGPT sintetiza os dilemas contemporâneos da governança digital: a tensão entre inovação e controle, entre liberdade e regulação, entre o benefício coletivo e o poder concentrado. Sua análise reforça o argumento central deste trabalho: a disputa pela regulação e pelo acesso aos dados tornou-se o novo terreno do poder global. E, enquanto os grandes atores estatais e corporativos competem pela liderança dessa nova fronteira tecnológica, a sociedade civil permanece distante dos debates que definirão o futuro da informação, da privacidade e da própria democracia digital.

5. Conclusão

A consolidação do capitalismo de vigilância, intensificada pelos sistemas de Inteligência Artificial e pelas dinâmicas geopolíticas entre grandes potências, revela uma urgência que não pode mais ser ignorada. A assimetria profunda entre quem coleta dados e quem é coletado produz riscos concretos à autonomia individual, à segurança informacional e à própria vitalidade democrática. Diante desse cenário, torna-se imprescindível que governos, instituições multilaterais, empresas e, sobretudo, a sociedade civil adotem medidas coordenadas que reduzam a opacidade dos fluxos de dados e ampliem mecanismos de transparência, responsabilidade e proteção de direitos.

Selecionar e implementar as opções políticas adequadas é decisivo para mitigar os custos, como vigilância abusiva, concentração de poder e erosão da privacidade, e, simultaneamente, maximizar benefícios como inovação responsável, segurança digital e fortalecimento da cidadania informada. Essas escolhas se alinham diretamente aos Objetivos de Desenvolvimento Sustentável, especialmente ao ODS 4 (Educação de Qualidade), ao promover alfabetização digital e consciência crítica; ao ODS 9 (Indústria, Inovação e Infraestrutura), ao incentivar tecnologias responsáveis; ao ODS 10 (Redução das Desigualdades), ao enfrentar assimetrias informacionais; ao ODS 16 (Paz, Justiça e Instituições Eficazes), ao fortalecer garantias democráticas; e ao ODS 17 (Parcerias e Meios de Implementação), ao demandar cooperação multissetorial e internacional para respostas efetivas.

Assim, o diagnóstico apresentado ao longo do trabalho conduz naturalmente às recomendações que seguem, voltadas a construir uma governança de dados que valorize direitos fundamentais e ofereça instrumentos concretos para que cidadãos, Estados e empresas possam atuar de forma mais equilibrada nesse novo ecossistema informacional.

6. Caminhos de cooperação e recomendações

As recomendações apresentadas a seguir têm como propósito orientar a implementação de ações concretas capazes de enfrentar o problema diagnosticado ao longo deste *policy brief*: a consolidação de um modelo global de poder baseado na coleta massiva de dados, intensificado por sistemas de Inteligência Artificial e reforçado pela disputa geopolítica entre grandes potências, em um contexto marcado pela baixa conscientização da sociedade civil. As medidas propostas constituem caminhos viáveis para mitigar assimetrias informacionais, ampliar a transparência das plataformas digitais, fortalecer mecanismos de governança ética e proteger direitos fundamentais, ao mesmo tempo em que contribuem para a construção de um ambiente digital mais seguro, democrático e alinhado aos Objetivos de Desenvolvimento Sustentável.

Expandir canais de participação ativa da sociedade civil na governança digital

A superação do atual modelo de poder digital, estruturado na exploração assimétrica de dados e na opacidade algorítmica, exige reconhecer a sociedade civil como beneficiária e principalmente como agente central da governança informacional. Para isso, recomenda-se a ampliação e institucionalização de canais formais de participação cidadã na formulação, monitoramento e revisão de políticas digitais.

Estados nacionais, conselhos regulatórios e organismos internacionais devem criar mecanismos permanentes de consulta pública, assembleias digitais deliberativas, observatórios de direitos digitais e conselhos multissetoriais com representação de organizações sociais, especialistas independentes, coletivos de tecnologia e grupos vulneráveis afetados de forma desproporcional pela vigilância algorítmica. Esses espaços devem ter poder real de influência, com capacidade de recomendar ajustes normativos, avaliar riscos sociais emergentes e acompanhar a

implementação de políticas de proteção de dados, transparência e accountability algorítmica.

O financiamento pode vir de fundos públicos destinados à participação democrática, de parcerias com universidades e de convênios com organizações internacionais voltadas à promoção de direitos humanos na era digital. Ao fortalecer a participação cidadã, essa recomendação reduz a distância entre governantes, plataformas e usuários, democratiza o debate tecnológico e mitiga a captura regulatória por grandes empresas. Além disso, contribui para reequilibrar a lógica do capitalismo de vigilância, ao reconhecer que os cidadãos, cujos dados alimentam sistemas de IA e modelos de negócios digitais, devem exercer poder ativo sobre a arquitetura regulatória que os afeta.

Estabelecer padrões internacionais mínimos para governança de dados e Inteligência Artificial

A construção de padrões mínimos globais é o primeiro passo para tornar a governança digital menos fragmentada e mais previsível. Estados nacionais, em articulação com a UNESCO, OECD e a ONU, devem priorizar a formulação de princípios universais referentes à transparência algorítmica, explicabilidade, minimização de coleta de dados, proteção de dados sensíveis e supervisão humana qualificada.

Esses padrões podem ser incorporados às legislações domésticas como instrumentos de *soft law*, o que permite adesão gradual mesmo de países com capacidades regulatórias limitadas. A capacitação técnica necessária pode ser viabilizada por fundos multilaterais destinados à transformação digital, além de parcerias público-privadas com centros de pesquisa e universidades especializadas em segurança algorítmica.

Ao estabelecer um núcleo normativo comum, essa recomendação contribui para reduzir assimetrias de poder entre grandes plataformas e Estados, garantindo à sociedade civil direitos mais claros e mecanismos mais consistentes de proteção diante da coleta massiva de dados.

Fortalecer mecanismos multilaterais de coordenação e supervisão digital

A rivalidade geopolítica entre Estados Unidos e China aprofundou a fragmentação normativa e tornou mais urgente a ampliação da capacidade institucional de organismos multilaterais. A ONU, o G20, o G7 e a OECD devem ampliar equipes técnicas, fortalecer comitês especializados e criar canais permanentes de supervisão sobre fluxos transnacionais de dados e sistemas de IA de alto risco. Essa coordenação multilateral pode incluir a publicação periódica de indicadores sobre práticas de vigilância digital, a criação de bases internacionais de dados para pesquisa independente, e a adoção de protocolos compartilhados de monitoramento de incidentes cibernéticos.

O financiamento pode vir de fundos existentes, como o UN Tech Envoy Fund, e de contribuições voluntárias de Estados e fundações internacionais comprometidas com segurança digital. O principal benefício dessa recomendação é aumentar a capacidade coletiva de fiscalização e reduzir o espaço de arbitragem regulatória explorado pelas big techs. Com isso, cria-se um ambiente internacional mais equilibrado, no qual padrões de responsabilidade corporativa não dependam exclusivamente da legislação de uma potência específica.

Promover interoperabilidade regulatória para mitigar a fragmentação digital

A fragmentação crescente do ecossistema digital global ameaça a segurança, a circulação de conhecimento e a própria arquitetura da Internet. Evitar esse cenário exige promover interoperabilidade regulatória, não no sentido de criar legislações idênticas, mas de construir pontes entre modelos distintos. Estados e organismos técnicos, como NIST, ISO e OECD, devem colaborar para desenvolver estruturas comuns de auditoria algorítmica, documentação técnica padronizada, métricas equivalentes de avaliação de risco e protocolos unificados de transparência.

Essa interoperabilidade reduz barreiras técnicas, facilita o diálogo entre legislações divergentes e torna mais difícil para empresas transnacionais se beneficiarem de jurisdições permissivas. O investimento necessário envolve tanto recursos públicos quanto contribuições do setor privado, que também se beneficia da previsibilidade gerada por padrões compatíveis. Para os cidadãos, o impacto é imediato: sistemas mais rastreáveis, decisões automatizadas mais explicáveis e redução da opacidade que caracteriza o capitalismo de vigilância.

Fortalecer educação digital crítica, alfabetização algorítmica e iniciativas de fact-checking

A sociedade civil deve ser tratada não como espectadora, mas como agente fundamental da governança digital. Por isso, recomenda-se que governos, universidades, escolas, veículos de mídia e organizações sociais desenvolvam programas de formação em educação digital crítica, alfabetização algorítmica e verificação de informações (*fact-checking*).

Esses programas podem ser implementados por meio de currículos escolares, campanhas públicas, oficinas comunitárias e consórcios com organizações independentes de verificação. O financiamento pode vir de fundos educacionais, editais internacionais de defesa da democracia e contrapartidas financeiras das próprias plataformas digitais, responsáveis por parte dos riscos informacionais que se busca mitigar.

Ao capacitar cidadãos a compreender o funcionamento dos algoritmos, identificar manipulações e reconhecer o valor de seus dados, essa recomendação contribui diretamente para reduzir a vulnerabilidade estrutural que sustenta o capitalismo de vigilância. Além disso, fortalece a resiliência democrática ao dificultar a disseminação de conteúdos enganosos amplificados por sistemas de recomendação opacos.

Ampliar a responsabilização das big techs por meio de transparência e auditorias independentes

O poder das big techs exige mecanismos de responsabilização capazes de transcender a legislação formal, especialmente enquanto não houver consenso regulatório internacional. Recomenda-se a criação de obrigações robustas de transparência, incluindo relatórios amplos sobre práticas de coleta, critérios de moderação, riscos algorítmicos e impactos sociais de sistemas automatizados.

Paralelamente, auditorias independentes conduzidas por centros de pesquisa, laboratórios externos e organizações técnicas devem tornar-se prática institucionalizada, com acesso controlado a modelos e bases de treinamento para

avaliar vieses, riscos de discriminação, vulnerabilidades de segurança e práticas de exploração de dados.

O financiamento dessas auditorias deve vir das próprias plataformas, sob um modelo de responsabilidade ampliada. Adicionalmente, índices públicos de transparência e rankings internacionais podem produzir pressão reputacional, mobilizando investidores e consumidores a exigir padrões éticos mais rigorosos. Ao aproximar empresas do escrutínio público, essa recomendação reduz a assimetria informacional que fundamenta o capitalismo de vigilância e fortalece a capacidade coletiva de supervisão digital.

7. Referências bibliográficas

AMNESTY INTERNATIONAL. “**I feel exposed**”: caught in TikTok’s surveillance web. London: Amnesty International, 2023. Disponível em: <https://www.amnesty.org/en/latest/research/2023/04/tiktok-surveillance-web/>.

Acesso em: 28 nov. 2025.

BBC NEWS. Italy temporarily bans ChatGPT over privacy concerns. **BBC News**, Londres, 31 mar. 2023. Disponível em: <https://www.bbc.com/news/technology-65139406> . Acesso em: 25 nov. 2025.

BROOKINGS INSTITUTION. KLONICK, Kate; WEST, Darrell M. TikTok shows why social media companies need more regulation. Washington, DC: Brookings Institution, 11 maio 2023. Disponível em: <https://www.brookings.edu/articles/tiktok-shows-why-social-media-companies-need-more-regulation/> . Acesso em: 30 nov. 2025.

BYUNG-CHUL HAN. **Psicopolítica**: o neoliberalismo e as novas técnicas de poder. Tradução de Maurício Liesen. Belo Horizonte: Âyiné, 2018.

CASTELLS, Manuel. **A sociedade em rede**. 19. ed. São Paulo: Paz e Terra, 2020. v. 1.

CENTER FOR AI AND DIGITAL POLICY (CAIDP). Comments of the Center for AI and Digital Policy to the U.S. Federal Trade Commission on commercial surveillance and data security. Washington, DC, 11 mar. 2024. Disponível em: https://downloads.regulations.gov/FTC-2024-0003-0262/attachment_1.pdf .

Acesso em: 14 set. 2025.

CROWDSTRIKE. **2025 CrowdStrike Global Threat Report**. Sunnyvale: CrowdStrike, 2025. Disponível em: <https://www.crowdstrike.com/global-threat-report/> . Acesso em: 11 out. 2025.

CSIS – CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES. **TikTok and the national security debate**. Washington, DC: Center for Strategic and International Studies, 2023. Disponível em: <https://www.csis.org/analysis/tiktok-and-national-security-debate> . Acesso em: 30 nov. 2025.

EUROPEAN PARLIAMENT. Children should be at least 16 to access social media, say MEPs. Bruxelas, 26 nov. 2025. Disponível em: <https://www.europarl.europa.eu/news/en/press-room/20251120IPR31496/children-should-be-at-least-16-to-access-social-media-say-meps> . Acesso em: 30 out. 2025.

EUROPEAN UNION. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). **Official Journal of the European Union**, L 119, p. 1-88, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> . Acesso em: 04 nov. 2025.

EUROPEAN UNION. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (**Artificial Intelligence Act**). **Official Journal of the European Union**, L 337, p. 1-120, 12 jul. 2024. Disponível em: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj> . Acesso em: 30 out. 2025.

HARARI, Yuval Noah. **Sapiens: uma breve história da humanidade**. 2. ed. São Paulo: Companhia das Letras, 2015.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Measuring digital development: Facts and Figures 2024**. Genebra: ITU, 2024. Disponível em: <https://www.itu.int/itu-d/reports/statistics/facts-figures-2024/> . Acesso em: 24 out. 2025.

MONOLITH: **The Recommendation System Behind TikTok**. LinkedIn, [S. l.], 14 abr. 2023. Publicado por Gantry ML. Disponível em:

<https://www.linkedin.com/pulse/monolith-recommendation-system-behind-tiktok-gantry-ml/>. Acesso em: 07 nov. 2025.

MOROZOV, Evgeny. **Big Tech**: a ascensão dos dados e a morte da política. Tradução de Claudio Marcondes. São Paulo: Ubu Editora, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Artificial Intelligence Risk Management Framework (AI RMF 1.0)**. Gaithersburg, MD: NIST, 2023. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ai/nist.ai.100-1.pdf> . Acesso em: 15 nov. 2025.

OECD – ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Digital Economy Outlook 2024** (Volume 1): Embracing the Technology Frontier. Paris: OECD Publishing, 2024. Disponível em: <https://doi.org/10.1787/a1689dc5-en> . Acesso em: 17 set. 2025.

OECD – ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Digital Economy Outlook 2024** (Volume 2): Strengthening Connectivity, Innovation and Trust. Paris: OECD Publishing, 2024. Disponível em: <https://doi.org/10.1787/e38f5db7-en> . Acesso em: 15 nov. 2025.

OECD – ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **Recommendation of the Council on Artificial Intelligence**. Paris: OECD, 2019. (Updated 2024). Disponível em: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> . Acesso em: 22 out. 2025.

OECD – ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD.AI Policy Observatory**. Paris: OECD, 2024. Disponível em: <https://oecd.ai/> . Acesso em: 11 out. 2025.

PEOPLE. Is TikTok getting banned on April 5? Here's why the app's future is up in the air. People, Nova York, 15 mar. 2025. Disponível em: <https://people.com/will-tiktok-be-banned-april-5-11697283/> . Acesso em: 25 nov. 2025.

PEW RESEARCH CENTER. Fewer Americans now support a TikTok ban, see the platform as a national security threat than in spring 2023. Washington, DC, 25 mar. 2025. Disponível em: <https://www.pewresearch.org/short-reads/2025/03/25/fewer-americans-now-support-tiktok-ban-see-the-platform-as-a-national-security-threat-than-in-spring-2023/> . Acesso em: 06 out. 2025.

STANFORD UNIVERSITY. **Artificial Intelligence Index Report 2024**. Stanford, CA: Stanford Institute for Human-Centered Artificial Intelligence, 2024. Disponível em: <https://aiindex.stanford.edu/report/> . Acesso em: 13 nov. 2025.

STATE COUNCIL (People's Republic of China). **New Generation Artificial Intelligence Development Plan**. Beijing: State Council, 2017. Disponível em: http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm . Acesso em: 28 set. 2025.

SYNERGY RESEARCH GROUP. Hyperscale data centers hit the thousand mark; total capacity is doubling every four years. **Synergy Research Group**, 2024. Disponível em: <https://www.srgresearch.com/articles/hyperscale-data-centers-hit-the-thousand-mark-total-capacity-is-doubling-every-four-years> . Acesso em: 30 out. 2025.

TELEGEOGRAPHY. **Submarine Cable Map 2024**. Washington, DC: TeleGeography, 2024. Disponível em: <https://www.submarinecablemap.com/> . Acesso em: 05 nov. 2025.

UBS EVIDENCE LAB. **UBS Evidence Lab: Generative AI – early economic impacts**. Zurique: UBS, 2023. Disponível em: <https://www.ubs.com/global/en/investment-bank/insights-and-data/generative-ai-2023.html> . Acesso em: 27 out. 2025.

UNCTAD – UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Digital Economy Report 2024: Technology, Trust, and Transformation**. Genebra: United Nations, 2024. Disponível em: <https://unctad.org/publication/digital-economy-report-2024-technology-trust-and-transformation> . Acesso em: 27 set. 2025.

UNESCO. Guidelines for the Governance of Digital Platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach. Paris: UNESCO Publishing, 2023. Disponível em: <https://www.unesco.org/en/internet-trust/guidelines> . Acesso em: 24 nov. 2025.

UNESCO. **Recommendation on the Ethics of Artificial Intelligence**. Paris: UNESCO, 2021. Disponível em: <https://unesdoc.unesco.org/ark:/48223/pf0000381137> . Acesso em: 02 nov. 2025.

UNITED NATIONS GENERAL ASSEMBLY. A/RES/78/265 – Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development. New York: United Nations, 21 mar. 2024. Disponível em: <https://digitallibrary.un.org/record/4043244> . Acesso em: 11 out. 2025.

UNITED NATIONS GENERAL ASSEMBLY. A/RES/78/311 – Enhancing international cooperation on capacity-building of artificial intelligence. New York: United Nations, 1 jul. 2024. Disponível em: <https://docs.un.org/en/A/res/78/311> . Acesso em: 13 nov. 2025.

UNITED NATIONS GENERAL ASSEMBLY. A/RES/79/239 – Artificial intelligence in the military domain and its implications for international peace and security. New York: United Nations, 24 dez. 2024. Disponível em: <https://docs.un.org/en/A/RES/79/239> . Acesso em: 22 nov. 2025.

UNITED STATES. **Protecting Americans from Foreign Adversary Controlled Applications Act**, Pub. L. No. 118-50, 2024. Disponível em: <https://www.congress.gov/bill/118th-congress/house-bill/7521/text> . Acesso em: 11 out. 2025.

WORLD BANK. **World Development Report 2021: Data for Better Lives**. Washington, DC: World Bank, 2021. Disponível em: <https://www.worldbank.org/en/publication/wdr2021> . Acesso em: 19 nov. 2025.

WORLD ECONOMIC FORUM. **Global Risks Report 2024**. Genebra: World Economic Forum, 2024. Disponível em: <https://www.weforum.org/reports/global-risks-report-2024/> . Acesso em: 15 set. 2025.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.