DIREITO & POLÍTICA

Direito e Política, vol. 21, n. 1, 2026

CIBERATAQUES, DESINFORMAÇÃO E GOVERNANÇA ALGORÍTMICA NA ERA DA SOBERANIA DIGITAL

Tiago Negrão Andrade

Maria Cristina Gobbi

Contextualização: A governança de fluxos informacionais e infraestruturas digitais (5G, IA) redefine soberania, segurança e democracia no capitalismo de dados, expondo vulnerabilidades a ciberataques e desinformação.

Objetivos: Analisar como essas infraestruturas articulam ciberataques, desinformação e governança algorítmica, reconfigurando soberania, democracia, privacidade e regimes de verdade.

Método: Pesquisa qualitativa e documental, com análise temática e crítica do discurso em fontes de organizações internacionais, governos, literatura acadêmica e imprensa.

Resultado: Ciberataques a infraestruturas críticas evidenciam a guerra no capitalismo de dados. Redes 5G ampliam vetores de ataque. Desinformação opera como guerra epistêmica, monetizando atenção e corroendo consensos democráticos. Governança algorítmica privada impõe colonialidade digital e desigualdades informacionais. O capitalismo de vigilância captura comportamentos e aprofunda assimetrias cognitivas. Conclui-se que a crise da governança digital requer governança tecnopolítica global em justiça epistêmica, soberania informacional e alfabetização digital crítica.

Palavras-chave: Infraestruturas Digitais; Ciberataques; Desinformação; Governança Algorítmica; Soberania Digital; Capitalismo de Dados.

CYBERATTACKS, DISINFORMATION AND ALGORITHMIC GOVERNANCE IN THE DIGITAL SOVEREIGNTY

Contextualization: The governance of informational flows and digital infrastructures (5G, AI) redefines sovereignty, security, and democracy under data capitalism, exposing vulnerabilities to cyberattacks and disinformation

Objectives: To analyze how these infrastructures orchestrate cyberattacks, disinformation, and algorithmic governance, thereby reconfiguring sovereignty, democracy, privacy, and regimes of truth.

Methodology: A qualitative, documentary study employing thematic analysis and critical discourse analysis on sources from international organizations, governments, academic literature, and the press.

Results: Cyberattacks targeting critical infrastructures reveal a form of warfare within data capitalism. 5G networks expand attack vectors. Disinformation functions as an epistemic war, monetizing attention and eroding democratic consensus. Private algorithmic governance imposes digital coloniality and informational inequalities. Surveillance capitalism captures behavior and deepens cognitive asymmetries. It follows that the crisis of digital governance demands a global techno-political governance founded on epistemic justice, informational sovereignty, and critical digital literacy.

Keywords: Nullity; Voidability; Functional Analysis; Succession Planning; Succession Pact.

CIBERATAQUES, DESINFORMACIÓN Y GOBERNANZA ALGORÍTMICA EN LA ERA DIGITAL

Contextualización: La gobernanza de los flujos informacionales e infraestructuras digitales (5G, IA) redefine la soberanía, seguridad y democracia en el capitalismo de datos, exponiendo vulnerabilidades a ciberataques y desinformación.

Objectivos: Analizar cómo estas infraestructuras articulan ciberataques, desinformación y gobernanza algorítmica, reconfigurando soberanía, democracia, privacidad y regímenes de la verdad.

Método: Estudio cualitativo y documental, con análisis temático y análisis crítico del discurso en fuentes de organizaciones internacionales, gobiernos, literatura académica y prensa.

Resultados: Los ciberataques a infraestructuras críticas evidencian una forma de guerra en el capitalismo de datos. Las redes 5G amplían los vectores de ataque. La desinformación opera como guerra epistémica, monetizando la atención y erosionando el consenso democrático. La gobernanza algorítmica privada impone colonialidad digital y desigualdades informacionales. El capitalismo de vigilancia captura comportamientos y profundiza las asimetrías cognitivas. Se concluye que la crisis de la gobernanza digital requiere una gobernanza tecnopolítica global basada en justicia epistémica, soberanía informacional y alfabetización digital crítica.

Palabras clave: Infraestructuras Digitales; Ciberataques; Desinformación; Gobernanza Algorítmica; Soberanía Digital; Capitalismo de Datos.

INTRODUÇÃO

A disputa contemporânea pela governança dos fluxos informacionais, dos sistemas algorítmicos e das infraestruturas digitais redefine, de maneira estrutural, os fundamentos da soberania, da segurança, da democracia e da própria arquitetura epistêmica das sociedades. Na era do capitalismo de dados e da hiperconectividade, a informação torna-se um vetor central de poder geopolítico, de controle social e de dominação econômica, conforme já alertava Zuboff[1] ao teorizar o conceito de "capitalismo de vigilância". A articulação entre big data, algoritmos e infraestruturas computacionais transforma o espaço digital em um campo estratégico de disputa por hegemonia.

Estudos da European Commission e da ENISA indicam que, até 2030, o volume de dados globais deve ultrapassar 180 zettabytes[2]. Com a proliferação de redes 5G, dispositivos IoT e sistemas de inteligência artificial, cresce a dependência estrutural de cidadãos, empresas e governos dessas infraestruturas. Paralelamente, verifica-se a intensificação de ataques cibernéticos contra setores estratégicos — como energia, saúde e finanças —, evidenciando o deslocamento da guerra para o domínio digital[3].

A transformação ontológica da esfera digital exige uma abordagem interdisciplinar. O conceito de netwar, formulado por Arquilla e Ronfeldt, já antecipava o papel das redes na guerra contemporânea[4]. Clarke e Knake[5] reafirmam essa virada ao equiparar a guerra cibernética às guerras tradicionais, destacando seu potencial de desestabilizar Estados inteiros[6]. A esses elementos soma-se a análise de Rid sobre a evolução dos ataques cibernéticos como instrumentos de guerra informacional e econômica[7].

No campo epistêmico, Floridi[8] propõe que não vivemos apenas uma crise

---

[1] ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. New York: PublicAffairs, 2019.

[2] EUROPEAN COMMISSION. **Shaping Europe's Digital Future**. Brussels, 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/digital-compass. Acesso em: 4 jun. 2025.

[3] ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. *ENISA Threat Landscape 2020:* **Cyber Attacks Becoming More Sophisticated, Targeted, Widespread.** 2020. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020. Acesso em: 4 jun. 2025.

[4] CISA – U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two** *Years.* 2023. Disponível em: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. Acesso em: 4 jun. 2025.

[5] CLARKE, Richard A.; KNAKE, Robert K. Cyber War: **The Next Threat to National Security and What to Do About It**. New York: HarperCollins, 2010.

[6] ARCHILLA, John; RONFELDT, David. **The Advent of Netwar.** Santa Monica: RAND Corporation, 1996. Disponível em: https://www.rand.org/pubs/monograph_reports/MR789.html . Acesso em: 4 jun. 2025.

[7] CLARKE, Richard A.; KNAKE, Robert K. Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins, 2010.

[8] FLORIDI, Luciano. **The Ethics of Information**. Oxford: Oxford University Press, 2013.

informacional, mas uma reconfiguração da própria ontologia da realidade mediada pela infosfera[9]. Esse deslocamento exige uma crítica das formas de poder algorítmico e das estruturas de governança digital que moldam os regimes de verdade e subjetividade[10].

Este artigo tem como objeto os regimes sociotécnicos que articulam ciberataques, manipulação informacional, governança algorítmica e transformação ontológica da esfera pública. Serão analisadas as infraestruturas digitais hiperconectadas — redes 5G, sistemas de IA, data centers, satélites e plataformas — como dispositivos epistêmicos, econômicos e geopolíticos. Diferentemente de abordagens técnicas, propomos uma leitura crítica centrada nas disputas por hegemonia, soberania digital e justiça epistêmica.

As perguntas norteadoras da pesquisa são: (i) de que forma os ciberataques e a desinformação participam da guerra híbrida digital contemporânea? (ii) como os sistemas algorítmicos reconfiguram soberanias e regimes de governança? e (iii) quais os impactos dessa nova ecologia informacional sobre democracia, agência subjetiva e regimes de verdade?

1. METODOLOGIA

Este estudo adota uma abordagem qualitativa, teórica, documental e crítica, ancorada em vertentes da economia política dos dados, da análise crítica do discurso e da governamentalidade digital, com o intuito de mapear e problematizar as disputas epistêmicas e geopolíticas que permeiam os regimes sociotécnicos contemporâneos. Para tanto, foram coletados documentos institucionais, relatórios oficiais de agências governamentais e multilaterais, legislações nacionais e internacionais, bem como publicações acadêmicas — abrangendo o período de 2010 a 2025 — por meio de consultas a bases de dados como Scopus, Web of Science, Redalyc e SciELO. A seleção do material baseou-se em descritores relacionados a ciberataques, infraestrutura digital, desinformação, governança algorítmica e soberania informacional, aplicando critérios de inclusão que priorizaram estudos que demonstrassem repercussão direta sobre disputas de poder informacional e crítica aos modelos de regulação existentes, enquanto trabalhos que abordassem exclusivamente aspectos técnicos sem vínculo com dimensões político-econômicas foram excluídos. Na etapa analítica, realizou-se codificação manual e análise temática dos textos, enfatizando práticas discursivas e normativas que revelam contradições entre imperativos de segurança cibernética e princípios de justiça epistêmica; simultaneamente, aplicou-se análise crítica do discurso para identificar como

[9] RID, Thomas. *Active Measures:* **The Secret History of Disinformation and Political Warfare.** New York: Farrar, Straus and Giroux, 2020.

[10] UNESCO. **Recommendation on the Ethics of Artificial Intelligence**. Paris, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137. Acesso em: 4 jun. 2025.

narrativas oficiais e midiáticas legitimam ou contestam políticas de controle digital. Com essa estratégia, busca-se compreender como as infraestruturas digitais se constituem como dispositivos de poder e como as tensões entre soberania nacional e soberania informacional emergem dos embates entre grandes corporações tecnológicas, Estados e atores sociais, revelando as potencialidades e limitações das respostas regulatórias vigentes.

2. RESULTADOS E DISCUSSÃO

A apresentação dos achados revela uma articulação dos principais vetores analíticos identificados no estudo, de modo que as evidências sobre ataques a infraestruturas críticas se entrelaçam com as dinâmicas de desinformação e com as configurações de governança algorítmica, evidenciando implicações tanto no plano teórico quanto nas esferas social, econômica e política. A partir dessa tessitura, reflete-se sobre como cada dimensão — desde as formas de subversão de redes 5G até os mecanismos de modulação cognitiva em plataformas digitais — dialoga com os desafios e contradições inerentes ao capitalismo de dados, enquanto se problematizam as estratégias regulatórias vigentes e se exploram possíveis avanços em termos de justiça epistêmica e soberania informacional. Ao considerar as repercussões tecnológicas, culturais e geopolíticas dos fenômenos analisados, as interpretações aqui expostas estabelecem uma ponte crítica que destaca a relevância de repensar as lógicas de poder algorítmico e os paradigmas de segurança digital, sinalizando, em última instância, as potencialidades e limites de cenários alternativos para a governança informacional.

2.1 Ciberataques, infraestruturas críticas e geopolítiga digital no ecossistema 5G

Os ciberataques contemporâneos não constituem apenas ameaças técnicas a sistemas computacionais, mas expressam uma reconfiguração das infraestruturas críticas como arenas de disputa geopolítica, onde o controle informacional opera como instrumento de poder soberano e de desestabilização interestatal[11]. A interdependência entre redes digitais e setores estratégicos — como energia, transporte e finanças — torna as infraestruturas vulneráveis não apenas a falhas técnicas, mas à ação intencional de atores estatais e paraestatais, reconfigurando o campo da segurança internacional.

O ataque à Colonial Pipeline, nos Estados Unidos, exemplifica como a guerra digital pode interromper cadeias logísticas e gerar efeitos econômicos imediatos, demonstrando

[11] RID, Thomas. *Active Measures:* **The Secret History of Disinformation and Political Warfare.** New York: Farrar, Straus and Giroux, 2020.

que a soberania territorial depende crescentemente da soberania sobre os fluxos de dados e da integridade das redes digitais[12]. A análise institucional realizada pela CISA expõe os limites das abordagens reativas à segurança cibernética e destaca a necessidade de políticas de ciberresiliência multissetoriais, integrando regulação, tecnologia e governança cooperativa[13].

Estudos recentes demonstram que a própria arquitetura fragmentada do 5G amplia a superfície de ataque em infraestrutura crítica ao possibilitar penetrações quase simultâneas em múltiplos sistemas interdependentes, como hospitais conectados, redes de distribuição de energia e sistemas logísticos inteligentes. Dados de 2024 apontam que incidentes envolvendo redes 5G tiveram aumento de 65 % em relação ao ciclo anterior, sendo responsáveis por interrupções prolongadas em centros hospitalares na Alemanha e sabotagens em subestações de energia nos Estados Unidos, desencadeando quedas em cascata que afetaram não apenas sistemas técnicos, mas também serviços de emergência e cadeias de suprimento. Essa elevação de risco corrobora a percepção de que, para além da latência e do throughput, o 5G consolida-se como um vetor geopolítico central, onde atores estatais e paraestatais podem explorar vulnerabilidades de forma seletiva para pressionar governos ou desestabilizar adversários econômicos e estratégicos[14].

Na América Latina, o caso do sistema bancário mexicano revelou como operações de origem desconhecida podem comprometer setores inteiros da economia, provocando respostas urgentes de instituições centrais e evidenciando a assimetria de capacidades cibernéticas entre o Norte e o Sul Global[15]. Esses ataques não são meramente técnicas de intrusão, mas formas de guerra informacional e econômica, frequentemente articuladas com interesses geopolíticos e experimentações tecnopolíticas.

Na Europa, as recorrentes invasões digitais ao parlamento alemão e aos servidores governamentais — atribuídas a grupos associados ao Kremlin — revelam o uso sistemático da espionagem digital como estratégia de desestabilização democrática e

---

[12] ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

[13] CISA – U.S. CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. *The Attack on Colonial Pipeline:* **What We've Learned & What We've Done Over the Past Two Years**. 2023. Disponível em: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. Acesso em: 4 jun. 2025.

[14] NEGRÃO DE ANDRADE et al. Cybersecurity in the Digital Era: Geopolitical Impacts and Structural Challenges. **IOSR Journal of Humanities and Social Science (IOSR-JHSS)**, v. 30, n. 1, ser. 6, p. 30–44, jan. 2025a. DOI: 10.9790/0837-3001063044.

[15] BLOOMBERG. **Mexico tells banks to take steps to guard against suspected hack.** Bloomberg, 30 abr. 2018. Disponível em: https://www.bloomberg.com/news/articles/2018-04-30/mexico-tells-banks-to-take-steps-to-guard-against-suspected-hack. Acesso em: 4 jun. 2025.

manipulação eleitoral[16]. Essa militarização do ciberespaço altera os parâmetros tradicionais da soberania, pois os ataques não requerem presença física nem declaratória: operam na opacidade algorítmica, na sobreposição entre público e privado, e na temporalidade acelerada dos dados.

A guerra informacional contemporânea, portanto, não se limita à desinformação simbólica: incide diretamente sobre as condições materiais da vida social, seja ao sabotar serviços essenciais, seja ao capturar plataformas de infraestrutura crítica, como provedores de nuvem, redes 5G e sistemas de gestão urbana[17]. O próprio conceito de soberania se desloca, passando a ser definido pela capacidade de controle técnico, normativo e epistêmico sobre as redes informacionais[18].

A disputa pelo fornecimento de componentes de 5G também se reflete em sanções comerciais e retaliações que afetam a integridade das cadeias globais de suprimento. Em particular, a imposição de restrições dos Estados Unidos à Huawei em 2019 levou à reconfiguração completa de contratos públicos de infraestrutura em países da Europa e da Ásia, resultando em atrasos de até 18 meses na expansão de redes 5G e em custos adicionais estimados em bilhões de dólares. Esse movimento evidenciou que a "guerra comercial do 5G" não é somente econômica, mas se converte em instrumento de pressão geopolítica, pois a fragmentação imposta pelos embargos força cada Estado a optar entre alinhamento estratégico – com risco de limitação tecnológica – ou dependência de fornecedores alternativos, mas menos maduros tecnologicamente[19].

Diante disso, a União Europeia tem buscado reforçar suas infraestruturas digitais por meio da integração entre regulação tecnológica, inteligência artificial confiável e defesa cibernética, conforme delineado na agenda "Shaping Europe's Digital Future" [20]. Contudo, tais estratégias permanecem atravessadas por assimetrias estruturais globais, que colocam países do Sul em posição periférica nas cadeias de produção tecnológica e nos circuitos decisórios sobre cibersegurança internacional[21].

---

[16] THE GUARDIAN. **Watch out, Europe. Germany is top of Russian hackers' list. The Guardian**, 13 jan. 2017. Disponível em: https://www.theguardian.com/commentisfree/2017/jan/13/europe-germany-russian-hackers-bundestag-angela-merkel-election. Acesso em: 4 jun. 2025.

[17] ARCHILLA, John; RONFELDT, David. **The Advent of Netwar. Santa Monica: RAND Corporation, 1996.** Disponível em: https://www.rand.org/pubs/monograph_reports/MR789.html. Acesso em: 4 jun. 2025.

[18] FLORIDI, Luciano. **The Ethics of Information.** Oxford: Oxford University Press, 2013.

[19] NEGRÃO DE ANDRADE et al. The Trade War Between China And The USA And The Geopolitical Impacts Of The 5G. **IOSR Journal of Humanities and Social Science (IOSR-JHSS)**, v. 30, n. 1, ser. 6, p. 21–29, jan. 2025b. DOI: 10.9790/0837-3001062129.

[20] EUROPEAN COMMISSION. **Shaping Europe's Digital Future**. Brussels, 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/digital-compass. Acesso em: 4 jun. 2025.

[21] UNESCO. **Recommendation on the Ethics of Artificial Intelligence.** Paris, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137. Acesso em: 4 jun. 2025.

2.2 Desinformação, manipulação cognitiva e guerra epistêmica no capitalismo de dados

A desinformação que circula sob a aparência de notícia não constitui um simples desvio factual ou ruído na comunicação pública, mas opera como dispositivo estruturante de uma violência simbólica que reorganiza regimes de visibilidade, reconhecimento e autoridade discursiva[22]. Ao produzir efeitos concretos sobre os sujeitos que podem ou não ocupar o lugar da verdade, a desinformação articula-se à gramática algorítmica das plataformas, modulando afetos, crenças e disposições ideológicas em larga escala[23].

Como propõe Bourdieu, a violência simbólica atua por meio da naturalização das estruturas de dominação, incorporando sentidos e hierarquias sem que pareçam arbitrárias[24]. Nas plataformas digitais, essa violência é amplificada por sistemas de recomendação que privilegiam conteúdos polarizantes e performativos, convertendo atenção em capital político, econômico e cultural. A verdade deixa de ser um critério regulador e passa a ser subordinada à lógica da viralização, do engajamento e da disputa por relevância algorítmica.

Foucault já havia demonstrado que os regimes de verdade são construídos historicamente por redes de poder e saber, que delimitam o que pode ser dito, quem pode dizer e em que condições[25]. No atual contexto tecnopolítico, essas redes tornam-se infraestruturais, inscritas em bases de dados, ontologias de classificação, sistemas de inferência e fluxos invisíveis de modulação informacional. A desinformação, nesse cenário, não é apenas conteúdo falso, mas o sintoma de um regime de produção de sentido colonizado por plataformas.

Esse fenômeno é ainda mais grave quando observamos seus efeitos sobre grupos historicamente marginalizados. Estudo conduzido pela Universidade de Michigan revela que usuários racializados, especialmente pessoas negras, são sistematicamente "shadowbanned" — ou seja, têm sua visibilidade restringida sem aviso ou justificativa, em nome de padrões automatizados de moderação[26]. Trata-se de uma reconfiguração cibernética da exclusão social, onde o silenciamento se dá não pela censura direta, mas pelo desaparecimento algorítmico.

---

[22] BOURDIEU, Pierre. **A dominação masculina.** Rio de Janeiro: Bertrand Brasil, 1998

[23] NOBLE, Safiya Umoja. **Algorithms of Oppression: How Search Engines Reinforce Racism.** New York: NYU Press, 2018. Disponível em: https://doi.org/10.2307/j.ctt1pwt9w5. Acesso em: 4 jun. 2025.

[24] BOURDIEU, Pierre. **O poder simbólico**. Rio de Janeiro: Bertrand Brasil, 2001.

[25] FOUCAULT, Michel. **Vigiar e Punir: Nascimento da Prisão**. 17. ed. Petrópolis: Vozes, 1996.

[26] UNIVERSITY OF MICHIGAN. **Study looks at 'shadowbanning' of marginalized social media users**. 2023. Disponível em: https://record.umich.edu/articles/study-looks-at-shadowbanning-of-marginalized-social-media-users/. Acesso em: 4 jun. 2025.

Essas dinâmicas não operam de forma neutra: elas replicam e reforçam estruturas de desigualdade racial, de gênero e territorial que já operam no mundo offline. Segundo Simone Browne, o racismo informacional e a vigilância algorítmica são extensões digitais das práticas de controle e policiamento que historicamente incidiram sobre os corpos negros[27]. A desinformação, assim, não é apenas uma distorção, mas uma forma de epistemicídio — uma supressão sistemática de saberes, vozes e experiências.

Por isso, pensar a desinformação exige ir além das soluções técnicas (como checagens ou remoções) e enfrentar as raízes estruturais da exclusão cognitiva e discursiva. Como aponta Ruha Benjamin, é preciso deslocar o foco do que os algoritmos fazem para quem eles servem, questionando os sistemas que os produzem, os dados que os alimentam e os futuros que silenciam[28].

2.3 Governança, soberania digital e geopolítica das infraestruturas algorítmicas

No cenário contemporâneo, a governança digital e a disputa pela soberania informacional não são fenômenos acessórios, mas sim a linha de frente das reconfigurações geopolíticas, econômicas e epistêmicas que moldam o século XXI. A convergência entre hiperconectividade, plataformização, inteligência algorítmica e guerra informacional dá origem a uma nova gramática do poder, na qual os fluxos de dados, as infraestruturas tecnológicas e os sistemas de governança algorítmica se tornam instrumentos estratégicos de dominação, controle e disputa hegemônica[29].

A centralidade desse processo é evidenciada por Wheeler, que argumenta que as infraestruturas digitais — em especial as redes 5G — passam a ser os novos territórios estratégicos da geopolítica global[30]. Ao problematizar a dependência tecnológica, Wheeler demonstra que a soberania nacional não pode mais ser pensada apenas nos termos clássicos do controle territorial, mas deve incorporar o domínio dos fluxos informacionais, das redes de comunicação e dos regimes algorítmicos que governam a circulação de dados, a infraestrutura econômica e, por extensão, a própria governabilidade dos Estados.

Essa leitura é aprofundada por Rid, que propõe que as infraestruturas informacionais operam como dispositivos de poder geopolítico, capazes de redefinir fronteiras não apenas no espaço físico, mas no espaço cognitivo, epistemológico e

[27] BROWNE, Simone. **Dark Matters: On the Surveillance of Blackness.** Durham: Duke University Press, 2015.

[28] BENJAMIN, Ruha. *Race* **After Technology: Abolitionist Tools for the New Jim Code**. Cambridge: Polity Press, 2019.

[29] ARCHILLA, John; RONFELDT, David. **The Advent of Netwar**. RAND Corporation, 1996. Disponível em: https://www.rand.org/pubs/monograph_reports/MR789.html

[30] WHEELER, Tom. **From Gutenberg to Google**: The History of Our Future. Brookings Institution Press, 2019. Disponível em: https://www.brookings.edu/books/from-gutenberg-to-google/

simbólico[31]. A arquitetura global da informação — centralizada em plataformas ocidentais e em infraestruturas sob domínio de Estados como os EUA e a China — torna-se, assim, uma forma de colonialidade digital, na qual os regimes de visibilidade, acesso e controle dos fluxos informacionais reproduzem e aprofundam assimetrias econômicas, epistêmicas e políticas no sistema-mundo.

Relatórios das Nações Unidas destacam como a ausência de marcos normativos robustos para a governança digital global permite que tensões geopolíticas se transmutem em disputas informacionais[32]. O caso da Crimeia evidencia que a captura das infraestruturas de informação — redes, satélites, data centers e plataformas — foi tão decisiva para a ocupação territorial quanto os movimentos militares convencionais, consolidando a lógica da guerra híbrida como paradigma estratégico das relações internacionais contemporâneas.

Zuboff[33] demonstra que plataformas digitais operam como "soberanias privadas extraterritoriais", definindo de forma unilateral os regimes de circulação de informações, os critérios de visibilidade e, consequentemente, os próprios limites da liberdade de expressão e do debate público. A governança algorítmica, nesse contexto, substitui o Estado como agente normativo, instaurando uma lógica na qual os imperativos econômicos da maximização do engajamento e da captura de dados se sobrepõem aos princípios da soberania, da democracia e dos direitos civis.

Floridi argumenta que, na ausência de marcos regulatórios epistêmicos e éticos, as infraestruturas digitais tornam-se vetores de opacidade algorítmica, precarizando não apenas os direitos individuais à privacidade, mas também as condições coletivas de produção de conhecimento, de deliberação pública e de construção de consensos mínimos[34]. O que está em jogo, portanto, não é apenas o controle da informação, mas a própria ontologia da realidade compartilhada na esfera pública digital.

Essa crise da governança informacional é diagnosticada nos relatórios da European Union Agency for Cybersecurity e da European Commission, que reconhecem que os marcos regulatórios europeus — mesmo os mais avançados — são insuficientes para enfrentar as dinâmicas extraterritoriais impostas pelas big techs[35]. A dificuldade de enforcement do GDPR, do Digital Services Act (DSA) e do Digital Markets Act (DMA)

[31] RID, Thomas. Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, 2020.

[32] UNITED NATIONS. Report of the Secretary-General on developments in the field of information and telecommunications in the context of international security. 2014. Disponível em: https://undocs.org/A/69/112

[33] ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**. New York: PublicAffairs, 2019.

[34] FLORIDI, Luciano. **The Ethics of Information.** Oxford: Oxford University Press, 2013.

[35] ENISA. **ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected.** Disponível em: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

evidencia que, enquanto a governança digital permanecer ancorada em estruturas jurídico-nacionais, será incapaz de confrontar corporações cujo modelo transcende fronteiras e sistemas legais.

O caráter colonial dessa arquitetura informacional é particularmente evidente nas relações entre o Norte Global e o Sul Global. Relatórios do Ministério do Meio Ambiente do Brasil documentam como campanhas de desinformação, moduladas por infraestruturas algorítmicas, foram utilizadas para desestabilizar percepções internacionais sobre os incêndios na Amazônia e intervir diretamente em políticas ambientais e diplomáticas[36]. Esse padrão também é verificado em processos eleitorais na Argentina, Turquia, Ucrânia e Colômbia, nos quais a instrumentalização de infraestruturas digitais comprometeu a autodeterminação democrática dos povos.

Além disso, legislações extraterritoriais como o Cloud Act e o Patriot Act impõem o acesso legal a dados armazenados fora do território estadunidense, comprometendo a soberania informacional de outros Estados[37]. Isso confirma que as disputas pela governança digital estruturam uma nova forma de imperialismo informacional, na qual o controle das infraestruturas de dados equivale ao controle dos fluxos econômicos, culturais e políticos.

Frente a esse cenário, as soluções propostas pelos próprios agentes do tecnocapitalismo — como modelos de autorregulação, códigos de conduta ética ou ferramentas de moderação automatizada — não passam de estratégias de captura da regulação. Como consequência, a ausência de uma governança algorítmica global eficaz aprofunda desigualdades epistêmicas e concentra o poder decisório nas mãos de poucos atores corporativos e estatais, corroendo os fundamentos da soberania, da democracia e da justiça informacional.

2.4 Ética, direitos, privacidade e ontologia algorítmica no capitalismo de dados

O aprofundamento das dinâmicas de captura de dados, vigilância algorítmica e plataformização não opera apenas no plano econômico, político ou geopolítico, mas impõe uma reconfiguração radical dos próprios fundamentos éticos, epistêmicos e ontológicos que sustentaram a modernidade. O regime sociotécnico emergente, centrado na extração massiva de dados, na engenharia comportamental preditiva e na opacidade algorítmica, produz não apenas novas formas de governança, mas uma nova gramática da

[36] LYNDON, R.; TSE, V.; MOORE, L.; MAY-HOBBS, M. **Desinformação no Brasil: Os incêndios na Amazônia de 2019 nas redes sociais.** In: MAIR, M.; MECKIN, R.; ELLIOT, M. (Eds.). Investigative Methods: An NCRM Innovation Collection. Southampton: National Centre for Research Methods, 2022. p. 44-53. DOI: 10.5258/NCRM/NCRM.00004547. Disponível em: https://eprints.ncrm.ac.uk/id/eprint/4547/.

[37] CLOUD Act. **Clarifying Lawful Overseas Use of Data Act**. 2018. Disponível em: https://www.congress.gov/bill/115th-congress/house-bill/4943

existência, da percepção e da própria possibilidade de agência dos sujeitos.

A captura de dados pessoais e sua transformação em matéria-prima para modelos de previsão comportamental estruturam uma arquitetura de controle social que compromete os princípios da autodeterminação, da privacidade e do consentimento informado. Ao sequestrar a subjetividade e convertê-la em ativo econômico, plataformas digitais passam a operar como dispositivos que modulam comportamentos, expectativas e decisões políticas.

Essa dinâmica de captura e monetização de vulnerabilidades extrapola a coleta passiva de dados e adentra o campo do "mercado clandestino" de exploits zero-day, no qual falhas ainda desconhecidas pelos fabricantes são negociadas a cifras que podem ultrapassar cinco milhões de dólares por transação. A comercialização dessas vulnerabilidades alimenta operações de espionagem e sabotagem que escalam a lógica do capitalismo de vigilância para uma esfera clandestina: agentes estatais, organizações criminais e hacktivistas podem adquirir exploits sem qualquer regulação ou prestação de contas, ampliando exponencialmente o risco de ataques direcionados a redes hospitalares, usinas de energia ou sistemas de transporte. A falta de consenso internacional sobre controles para esse mercado subterrâneo reforça a opacidade algorítmica e agrava as assimetrias de poder, uma vez que Estados mais poderosos podem obter ou produzir zero-days com maior facilidade, enquanto nações do Sul Global ficam à mercê de redes de inteligência estrangeiras, sem qualquer reparo jurídico ou ético[38].

A opacidade dos sistemas algorítmicos, muitas vezes justificada como necessidade técnica, revela-se uma estratégia de concentração informacional. Essa arquitetura intensifica assimetrias de poder e impede a deliberação pública transparente, criando infraestruturas opacas que afetam diretamente a cidadania, os direitos fundamentais e as possibilidades de resistência.

Evidências empíricas como o escândalo da Cambridge Analytica, que revelou o uso de dados obtidos sem consentimento para manipulação eleitoral em escala global, demonstram o impacto desse modelo na democracia. Relatórios como os da ENISA[39] e da Comissão Europeia[40] mostram que, mesmo com o avanço de marcos regulatórios como o GDPR e o DSA, as legislações continuam limitadas diante das dinâmicas extraterritoriais

[38] NEGRÃO DE ANDRADE et al. Zero-Day Vulnerabilities And The Clandestine Exploits Market: A Hermeneutic And Critical Approach. **IOSR Journal of Humanities and Social Science (IOSR-JHSS)**, v. 30, n. 1, ser. 7, p. 11–20, jan. 2025c. DOI: 10.9790/0837-3001071120.

[39] ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. ENISA **Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread**. 2020. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020. Acesso em: 4 jun. 2025.

[40] EUROPEAN COMMISSION. **Shaping Europe's Digital Future.** Brussels, 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/digital-compass. Acesso em: 4 jun. 2025.

e assimétricas das big techs.

A imposição de marcos jurídicos como o Cloud Act e o uso crescente de tecnologias de vigilância como o reconhecimento facial ampliam as ameaças à privacidade e à soberania digital, principalmente em países do Sul Global. Essas práticas impõem formas de vigilância generalizada e comprometem liberdades fundamentais.

Casos documentados por agências de segurança, como o ataque ao oleoduto Colonial Pipeline nos EUA[41], bem como operações de desinformação digital mapeadas na América Latina[42] [43], África[44] e Europa[45], evidenciam como os sistemas algorítmicos podem ser mobilizados como instrumentos de guerra híbrida, modulação cognitiva e sabotagem democrática.

Relatórios institucionais apontam ainda que o modelo de negócio baseado em engajamento e maximização da atenção é estruturalmente incompatível com a veracidade, a confiabilidade e o direito à informação de qualidade. A amplificação de conteúdos sensacionalistas, falsos ou polarizadores torna-se funcional a esse modelo, afetando diretamente os processos de construção da realidade compartilhada.

Nesse contexto, as tentativas tecnolibertárias de enfrentamento da crise — como blockchain, descentralização ou explicabilidade algorítmica — se mostram insuficientes, pois não abordam a concentração estrutural de poder informacional nem os impactos ontológicos do atual regime de dados.

A ausência de uma governança algorítmica global robusta acentua desigualdades históricas, sobretudo no Sul Global. Documentos da Comissão Europeia[46] e da UNESCO[47] alertam que a colonialidade digital impõe barreiras ao acesso, à representação e à

---

[41] CISA – U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years**. 2023. Disponível em: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. Acesso em: 4 jun. 2025.

[42] SCHWAB, Julia. **Social media and activism in the 2019/2020 Chilean social uprisings. 2020**. Undergraduate Honors Thesis – Department of International Studies, Seattle University, Seattle. Disponível em: https://scholarworks.seattleu.edu/intl-std-theses/3. Acesso em: 5 jun. 2025.

[43] FOLHA DE S.PAULO. **TSE falha no combate a fake news na campanha de primeiro turno.** Folha de S.Paulo, 29 out. 2018. Disponível em: https://www1.folha.uol.com.br/poder/2018/10/tse-falha-no-combate-a-fake-news-na-campanha-de-primeiro-turno.shtml . Acesso em: 4 jun. 2025.

[44] DISINFORMATION MONITOR. **What the 2023 Nigerian elections tell us about information manipulation.** [S. l.], 16 ago. 2023. Disponível em: https://disinfo.africa/what-the-2023-nigerian-elections-tell-us-about-information-manipulation-42d4dd70cbfd. Acesso em: 5 jun. 2025.

[45] THE GUARDIAN. **Watch out, Europe. Germany is top of Russian hackers' list.** The Guardian, 13 jan. 2017. Disponível em: https://www.theguardian.com/commentisfree/2017/jan/13/europe-germany-russian-hackers-bundestag-angela-merkel-election . Acesso em: 4 jun. 2025.

[46] EUROPEAN COMMISSION. **Shaping Europe's Digital Future.** Brussels, 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/digital-compass Acesso em: 4 jun. 2025.

[47] UNESCO. **Recommendation on the Ethics of Artificial Intelligence.** Paris, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137 . Acesso em: 4 jun. 2025.

proteção dos direitos informacionais, ampliando vulnerabilidades já existentes nos sistemas sociais, jurídicos e econômicos.

Portanto, a crise da governança algorítmica não pode ser interpretada apenas como um problema técnico ou setorial, mas como uma crise estrutural da modernidade, com impactos profundos sobre os fundamentos do contrato social, da soberania democrática e das condições de possibilidade da vida coletiva no século XXI.

3. SÍNTESE CONCLUSIVA

A análise das sessões — ciberataques às infraestruturas críticas, desinformação e guerra epistêmica, governança algorítmica e colonialidade digital, além dos desafios éticos, epistêmicos e ontológicos — revela que o ecossistema sociotécnico contemporâneo está estruturado por uma nova gramática de poder. Nessa nova configuração, soberania, segurança, democracia e regimes de verdade são profundamente reconfigurados pelas infraestruturas algorítmicas. O ciberespaço deixou de ser um domínio secundário ou paralelo e passou a constituir o campo central das disputas geopolíticas, econômicas e epistêmicas, onde se articulam estratégias de guerra híbrida, manipulação cognitiva, dominação informacional e reconfiguração das formas de governança.

Essa transição demonstra que a hiperconectividade viabilizada pelas redes de quinta geração, somada aos modelos extrativistas do capitalismo de dados, consolida um regime sociotécnico global que opera tanto pela captura econômica quanto pela colonização epistêmica e ontológica de sujeitos, instituições e Estados. A soberania digital, nesse contexto, revela-se não apenas vulnerável, mas sistematicamente corroída por arquiteturas informacionais privadas, extraterritoriais e opacas, orientadas por imperativos de lucro e controle comportamental, em detrimento de valores democráticos, éticos e epistêmicos.

As plataformas digitais, atuando como formas de soberania privada, transformam dados, atenção e cognição em ativos financeiros, ao mesmo tempo em que assumem funções historicamente atribuídas aos Estados, como a definição de regimes de visibilidade, a regulação das interações sociais e a imposição de normas discursivas. Esse processo reflete uma transformação ontológica, na qual os algoritmos não apenas mediam, mas produzem a realidade social, política e epistêmica.

A governança algorítmica global, marcada pela ausência de marcos jurídicos eficazes, pelo descompasso regulatório e pela captura das esferas pública e privada, aprofunda desigualdades históricas, reproduz formas de colonialidade digital e impõe desafios civilizatórios de natureza inédita.

A regulação das big techs, as propostas de soberania digital e os tratados internacionais existentes — como o GDPR, o DSA/DMA e o AI Act — representam esforços relevantes no campo normativo, mas revelam-se estruturalmente limitados diante da velocidade, da escala e da arquitetura extraterritorial das infraestruturas algorítmicas. Documentos como o *Shaping Europe's Digital Future* da Comissão Europeia evidenciam a intenção de fortalecer a autonomia digital do continente, mas reconhecem os desafios impostos pela assimetria informacional global[48].

A análise de relatórios internacionais, como o da ENISA sobre o panorama de ameaças cibernéticas[49] e os documentos da CISA sobre ataques a infraestruturas críticas[50], revela que os mecanismos de resposta continuam fragmentados, reativos e desarticulados frente à complexidade das ameaças informacionais contemporâneas. A experiência da União Europeia, embora robusta em termos de estrutura legal, ainda não se traduz em eficácia prática diante da lógica evasiva e opaca das plataformas globais.

Nesse sentido, torna-se evidente que o enfrentamento da crise da governança algorítmica requer respostas integradas que superem os marcos tradicionais da regulação econômica e da segurança cibernética. A UNESCO tem avançado nesse debate ao propor diretrizes éticas para a inteligência artificial com base em princípios de dignidade, transparência e justiça social[51]. Da mesma forma, a OCDE tem promovido iniciativas como a *Global Partnership on AI* com foco na construção de uma governança informacional planetária[52].

A soberania informacional e a justiça epistêmica exigem não apenas a reformulação das leis existentes, mas também a inclusão da alfabetização digital crítica como política de Estado, o fortalecimento de iniciativas multilaterais, e a consolidação de redes de cooperação internacional. O caso da Ucrânia[53],analisado pela OCDE, evidencia

---

[48] EUROPEAN COMMISSION. **Shaping Europe's Digital Future**. Brussels, 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/digital-compass. Acesso em: 4 jun. 2025.

[49] ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. *ENISA T***hreat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread.** 2020. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020. Acesso em: 4 jun. 2025.

[50] CISA – U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years**. 2023. Disponível em: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. Acesso em: 4 jun. 2025.

[51] UNESCO. **Recommendation on the Ethics of Artificial Intelligence.** Paris, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137. Acesso em: 4 jun. 2025.

[52] OECD. **Securing Democracy: Electoral Cybersecurity in Ukraine.** Paris: OECD, 2019. Disponível em: https://www.oecd.org/cyber/ukraine-electoral-cybersecurity-2019.pdf. Acesso em: 4 jun. 2025.

[53] OCDE. **Enhancing resilience by boosting digital business transformation in Ukraine.** Paris: OECD Publishing, 2024. Disponível em: https://www.oecd.org/en/publications/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_4b13b0bb-en.html. Acesso em: 5 jun. 2025.

como a articulação entre segurança cibernética, transformação digital e fortalecimento da soberania democrática pode gerar avanços significativos mesmo diante de ataques massivos. Através de políticas públicas integradas, o país investiu na digitalização de serviços governamentais, como o aplicativo Diia, e no fortalecimento da resiliência cibernética de pequenas e médias empresas, promovendo a continuidade institucional, a transparência e a confiança da população nas instituições democráticas, mesmo em um contexto de guerra e instabilidade.

4. LIMITAÇÕES DO ESTUDO E RECOMENDAÇÕES FUTURAS

Este estudo se baseou predominantemente na análise teórica, documental e em dados secundários, o que impõe limitações na obtenção de dados empíricos diretos sobre práticas internas das corporações tecnológicas, processos decisórios algorítmicos opacos e dinâmicas de ciberconflitos em tempo real. Além disso, a ênfase nas dinâmicas geopolíticas centradas em Europa, Estados Unidos e China limita, em certa medida, uma compreensão mais ampla dos impactos sobre regiões do Sul Global, cujas experiências de resistência, adaptação ou subversão dos regimes algorítmicos merecem maior aprofundamento.

Diante dessas limitações, recomenda-se que pesquisas futuras avancem na realização de estudos empíricos aplicados, incluindo auditorias algorítmicas independentes, etnografias digitais, análise forense de ciberataques e estudos comparativos entre marcos regulatórios de diferentes países e blocos econômicos. Além disso, é imperativo investigar as práticas de resistência, soberania tecnológica e inovação regulatória desenvolvidas por países do Sul Global, povos indígenas, comunidades periféricas e movimentos sociais, que frequentemente operam na fronteira entre vulnerabilidade e inovação epistêmica frente às dinâmicas de colonialidade digital. Por fim, sugere-se aprofundar os estudos interdisciplinares que integrem sociologia da tecnologia, filosofia da informação, economia política dos dados e estudos críticos de segurança cibernética para formulação de modelos alternativos de governança, regulação e justiça digital.

REFERENCIAS DAS FONTES CITADAS

ARCHILLA, John; RONFELDT, David. **The Advent of Netwar**. Santa Monica: RAND Corporation, 1996. Disponível em: https://www.rand.org/pubs/monograph_reports/MR789.html. Acesso em: 4 jun. 2025.

BENJAMIN, Ruha. Race After Technology: Abolitionist Tools for the New Jim Code. Cambridge: Polity Press, 2019.

BOURDIEU, Pierre. **A dominação masculina.** Rio de Janeiro: Bertrand Brasil, 1998.

BOURDIEU, Pierre. **O poder simbólico.** Rio de Janeiro: Bertrand Brasil, 2001.

BROWNE, Simone. **Dark Matters: On the Surveillance of Blackness.** Durham: Duke University Press, 2015.

CISA – U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. **The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two** Years. 2023. Disponível em: https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years. Acesso em: 4 jun. 2025.

CLARKE, Richard A.; KNAKE, Robert K. Cyber War: The Next Threat to National Security and What to Do About It. New York: HarperCollins, 2010.

CLOUD Act. **Clarifying Lawful Overseas Use of Data Act.** 2018. Disponível em: https://www.congress.gov/bill/115th-congress/house-bill/4943. Acesso em: 4 jun. 2025.

DISINFORMATION MONITOR. **What the 2023 Nigerian elections tell us about information manipulation.** [S. I.: s.n.], 16 ago. 2023. Disponível em: https://disinfo.africa/what-the-2023-nigerian-elections-tell-us-about-information-manipulation-42d4dd7. Acesso em: 4 jun. 2025.

ENISA – EUROPEAN UNION AGENCY FOR CYBERSECURITY. ENISA **Threat Landscape 2020! Cyber Attacks Becoming More Sophisticated, Targeted, Widespread.** 2020. Disponível em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020. Acesso em: 4 jun. 2025.

EUROPEAN COMMISSION. **Shaping Europe's Digital Future. Brussels,** 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/digital-compass. Acesso em: 4 jun. 2025.

FLORIDI, Luciano. **The Ethics of Information.** Oxford: Oxford University Press, 2013.

FOLHA DE S.PAULO. **TSE falha no combate a fake news na campanha de primeiro turno.** Folha de S.Paulo, 29 out. 2018. Disponível em: https://www1.folha.uol.com.br/poder/2018/10/rse-falha-no-combate-a-fake-news-na-campanha-de-pri. Acesso em: 4 jun. 2025.

FOUCAULT, Michel. **Vigiar e Punir: Nascimento da Prisão.** 17. ed. Petrópolis: Vozes, 1996.

LYNDON, R.; TSE, V.; MOORE, L.; MAY-HOBBS, M. **Desinformação no Brasil: Os incêndios na Amazônia de 2019 nas redes sociais. I**n: MAIR, M.; MECKIN, R.; ELLIOT, M. (Eds.). Investigative Methods: An NCRM Innovation Collection. Southampton: National Centre for Research Methods, 2022. p. 44–53. DOI: 10.5258/NCRM/NCRM.00004547. Disponível em: https://eprints.ncrm.ac.uk/id/eprint/4547/. Acesso em: 4 jun. 2025.

NEGRÃO DE ANDRADE et al. Cybersecurity in the Digital Era: Geopolitical Impacts and Structural Challenges. **IOSR Journal of Humanities and Social Science (IOSR-JHSS)**, v. 30, n. 1, ser. 6, p. 30–44, jan. 2025a. DOI: 10.9790/0837-3001063044.

NEGRÃO DE ANDRADE et al. The Trade War Between China And The USA And The Geopolitical Impacts Of The 5G. IOSR **Journal of Humanities and Social Science (IOSR-JHSS),** v. 30, n. 1, ser. 6, p. 21–29, jan. 2025b. DOI: 10.9790/0837-3001062129.

NEGRÃO DE ANDRADE et al. Zero-Day Vulnerabilities And The Clandestine Exploits Market: A Hermeneutic And Critical Approach. **IOSR Journal of Humanities and Social Science (IOSR-JHSS)**, v. 30, n. 1, ser. 7, p. 11–20, jan. 2025c. DOI: 10.9790/0837-3001071120.

NOBLE, Safiya Umoja. **Algorithms of Oppression: How Search Engines Reinforce Racism.** New York: NYU Press, 2018. Disponível em: https://doi.org/10.2307/j.ctt1pwt9w5. Acesso em: 4 jun. 2025.

OCDE. **Enhancing resilience by boosting digital business transformation in Ukraine.** Paris: OECD Publishing, 2024. Disponível em: https://www.oecd.org/en/publications/enhancing-resilience-by-boosting-digital-business-transformation. Acesso em: 4 jun. 2025.

OECD. **Securing Democracy: Electoral Cybersecurity in Ukraine.** Paris: OECD, 2019. Disponível em: https://www.oecd.org/cyber/ukraine-electoral-cybersecurity-2019.pdf. Acesso em: 4 jun. 2025.

RID, Thomas. Active Measures: **The Secret History of Disinformation and Political Warfare.** New York: Farrar, Straus and Giroux, 2020.

SCHWAB, Julia. **Social media and activism in the 2019/2020 Chilean social uprisings.** Undergraduate Honors Thesis – Department of International Studies, Seattle University, Seattle, 2020. Disponível em: https://scholarworks.seattleu.edu/intl-std-theses/3. Acesso em: 5 jun. 2025.

UNESCO. **Recommendation on the Ethics of Artificial Intelligence.** Paris, 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137. Acesso em: 4 jun. 2025.

UNITED NATIONS. Report of the Secretary-General on developments in the field of information and telecommunications in the context of international security. 2014. Disponível em: https://undocs.org/A/69/112. Acesso em: 4 jun. 2025.

UNIVERSITY OF MICHIGAN. **Study looks at 'shadowbanning' of marginalized social media users.** 2023. Disponível em: https://record.umich.edu/articles/study-looks-at-shadowbanning-of-marginalized-social-media-users/. Acesso em: 4 jun. 2025.

WHEELER, Tom. **From Gutenberg to Google: The History of Our Future.** Washington, D.C.: Brookings Institution Press, 2019.

ZUBOFF, Shoshana. **The Age of Surveillance Capitalism**: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

COMO CITAR

ANDRADE, Tiago Negrão; GOBBI, Maria Cristina. Ciberataques, desinformação e governança algorítmica na era da soberania digital. **Revista Direito e Política**. Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI, vº 21, nº1, 1º quadrimestre de 2026. Disponível em: https://periodicos.univali.br/index.php/rdp - ISSN 1980-7791. DOI: https://doi.org/10.14210/rdp.v21n1.p41-60

SOBRE OS AUTORES:

Tiago Negrão Andrade
Doutor em Mídia e Tecnologia pela FAAC - Faculdade de Arquitetura, Artes e Comunicação - Campus de Bauru, da Universidade Estadual Paulista "Júlio de Mesquita Filho". Graduado em Comunicação Social - Habilitação em Relação Pública pela Universidade de Sorocaba (UNISO).

Maria Cristina Gobbi
Bolsista de Produtividade em Pesquisa do CNPq. Pesquisadora Livre docente (RDIDP) em História da Comunicação e da Cultura Midiática na América Latina, professora da graduação em Jornalismo e dos Programas de Pós-Graduação em Comunicação (PPGCom) e em Mídia e Tecnologia (PPGMiT) da Universidade Estadual Paulista (UNESP), Faculdade de Arquitetura, Artes e Comunicação e Design (FAAC) e chefa do Departamento de Jornalismo (DJor) (2024-2026). E-mail: mcgobbi@terra.com.br; cristina.gobbi@unesp.br

Received: 06/06/2025
Approved: 06/02/2026

Recebido em: 06/06/2025
Aprovado em: 06/02/2026