

IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Naspolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFRS - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Ednilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Rubens Beçak; Aires Jose Rover; Ana Elisa Silva Fernandes Vieira – Florianópolis: CONPEDI, 2026.

Inclui bibliografia

ISBN: 978-65-5274-592-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, Processo e Justiça Social: o papel da jurisdição constitucional na efetivação de direitos

2. Direito. 3. Governança e novas tecnologias. IX Encontro Virtual do CONPEDI (2: 2026: Florianópolis, Brasil).

CDU: 34



IX ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

Os encontros nacionais do Conselho Nacional de Pesquisa e Pós-graduação em Direito (CONPEDI) têm se consolidado como referência na disseminação de pesquisas que abordam os novos fenômenos envolvendo o direito, e o Grupo de Trabalho "Direito, Governança e Novas Tecnologias" é um exemplo vivo desse compromisso. Nesta edição, o evento destacou-se não apenas pela qualidade dos trabalhos apresentados, mas pela presença de renomados professores pesquisadores em instigante debate com seus alunos de pós-graduação.

Como de praxe, houve uma diversidade muito grande de temas e abordagens. Numa tentativa de dar unidade temática e facilitar a compreensão dessa complexa teia de inovações, os coordenadores organizaram os artigos desta publicação em três grandes grupos de reflexão.

O primeiro bloco abordou o tema da "Inteligência Artificial, Viés Algorítmico e Responsabilidade Tecnológica". As reflexões apresentadas neste eixo evidenciam a tensão constante entre a rápida expansão da inteligência artificial - que transforma desde o papel da advocacia e o uso de "smart contracts" até a governança das plataformas digitais - e os profundos riscos sociais intrínsecos a essas tecnologias. Os debates trouxeram à tona denúncias contundentes sobre o racismo estrutural e algorítmico, demonstrando como projetos de cidades inteligentes e ferramentas de reconhecimento facial podem operar sob uma lógica de necropolítica se não houver um olhar crítico. Consequentemente, os pesquisadores debruçaram-se sobre a urgência de estabelecer novos marcos de regulação, modelos de responsabilidade civil e robustos mecanismos de "compliance" e segurança da informação para frear a discriminação e garantir proteção contratual.

destaque para a urgência de uma identidade digital segura e a afirmação de um Estatuto da Criança e do Adolescente (ECA) no ambiente virtual.

Por fim, o terceiro bloco englobou "Direitos Humanos, Processo Judicial, Economia Digital e Governança Institucional". Este eixo refletiu de forma abrangente as complexas interseções entre a Revolução 4.0 e a proteção da dignidade humana. Foram problematizados fenômenos contemporâneos alarmantes, como a precarização das relações na "gig economy", o abandono parental no ambiente virtual e a violação do direito ao esquecimento infantil decorrente do "oversharenting". Em paralelo a essas vulnerabilidades, os estudos investigaram a modernização das estruturas institucionais e econômicas. Discutiu-se desde a responsabilidade civil frente à tokenização e financeirização de terras no agronegócio, até o esforço contínuo para democratizar o sistema de justiça. Para isso, foram apresentadas análises valiosas sobre a implantação municipal do processo eletrônico, a aplicação do "design thinking" no direito e o aprimoramento da transparência e da participação democrática sob a ótica do direito comparado.

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno das respostas que o Direito precisa dar a uma realidade em constante e veloz transformação.

Enfim, os coordenadores do GT convidam os leitores para desfrutarem do teor integral dos artigos, expressando imensa gratidão pela participação dos autores pesquisadores desta edição.

Os Coordenadores

Prof. Dr. Aires José Rover, Universidade Federal de Santa Catarina

Prof. Dr. .Rubens Beçak, Universidade de São Paulo - USP

SOBERANIA DIGITAL E EMANCIPAÇÃO TECNOPOLÍTICA: DESAFIOS DO COLONIALISMO DE DADOS, DA CIDADANIA INSURGENTE E DA GOVERNANÇA DIGITAL AO ESTADO BRASILEIRO

DIGITAL SOVEREIGNTY AND TECHNOPOLITICAL EMANCIPATION: CHALLENGES OF DATA COLONIALISM, INSURGENT CITIZENSHIP, AND DIGITAL GOVERNANCE FOR THE BRAZILIAN STATE

Carine Labres ¹

Resumo

O artigo analisa a soberania digital como dimensão estratégica da democracia, da cidadania e da proteção dos direitos fundamentais na Era da Informação. Parte-se da constatação de que o avanço tecnológico e a captura massiva de dados inauguraram uma nova forma de colonialismo, denominada colonialismo digital, caracterizada pela dependência informacional de Estados e cidadãos em relação às grandes corporações transnacionais. A partir de abordagem qualitativa e revisão bibliográfica, o estudo discute três eixos principais: primeiro, a soberania estatal e a tensão entre autonomia informacional e capitalismo de vigilância; segundo, a democracia digital e a cidadania insurgente, compreendidas como práticas de resistência e emancipação tecnológica a partir das contribuições de Haraway, Nemer e Faustino e Lippold; e terceiro, os desafios da governança digital brasileira, com ênfase na neutralidade de rede, na proteção de dados e na construção de infraestruturas públicas digitais. Conclui-se que a consolidação do Estado Democrático de Direito no ciberespaço requer autonomia tecnológica, letramento digital e políticas inclusivas de governança, capazes de assegurar direitos fundamentais e reduzir desigualdades no ambiente digital.

Palavras-chave: Soberania digital, Cidadania insurgente, Governança digital, Colonialismo digital, Capitalismo de vigilância

Abstract/Resumen/Résumé

This article analyzes digital sovereignty as a strategic dimension of democracy, citizenship,

third, the challenges of Brazilian digital governance, with an emphasis on net neutrality, data protection, and the construction of public digital infrastructures. It concludes that the consolidation of the Democratic Rule of Law in cyberspace requires technological autonomy, digital literacy, and inclusive governance policies capable of ensuring fundamental rights and reducing inequalities in the digital environment.

Keywords/Palabras-claves/Mots-clés: Digital sovereignty, Insurgent citizenship, Digital colonialism, Digital governance, Surveillance capitalism

1. INTRODUÇÃO

A Era Digital acarretou mudanças significativas nas relações geopolíticas e sociais, em velocidade exponencial, condizente com sua matriz de desenvolvimento: a tecnologia, da qual resultam a internet e plataformas digitais. Atualmente, há uma relação indissociável entre tecnologia e desenvolvimento econômico e social, que faz emergir desafios à noção de soberania. As fronteiras entre o “mundo digital e mundo real” são cada vez mais invisíveis, desencadeando conflitos entre controle e liberdade, segurança e privacidade.

Isso evidencia o quão urgente se faz repensar a noção de soberania, pois transcende dimensões jurídicas e políticas, abrangendo a capacidade tecnológica e o controle informacional de dados, como instrumentos efetivos de proteção e exercício dos direitos fundamentais em ambiente digital. A internet e as plataformas digitais, por exemplo, configuram instrumentos centrais da geopolítica contemporânea, com capacidade de influenciar diretamente decisões soberanas. Ao concentrarem poder econômico, informacional e comunicacional, as corporações privadas exercem pressões que transcendem fronteiras e impactam áreas sensíveis como segurança nacional, cidadania, dinâmicas culturais e políticas econômicas.

Não há dúvidas de que tanto a geopolítica contemporânea como as relações sociais desenvolvidas entre os cidadãos são marcadas pela presença de algoritmos, redes virtuais e pela economia baseada em dados. Esses elementos, embora frequentemente celebrados como mecanismos de fortalecimento da cidadania e ampliação do acesso à informação, nem sempre produzem efeitos democratizantes. Para comunidades periféricas e historicamente marginalizadas, a promessa de inclusão digital revela-se parcial, seletiva e, em muitos casos, excludente. Em vez de promover uma cidadania plena, a tecnologia opera com filtros invisíveis que regulam quem pode ser visto, ouvido e reconhecido. Trata-se de uma cidadania moldada por estruturas de poder que controlam o acesso, a visibilidade e o valor das vozes subalternizadas.

Nesse cenário, o investimento do Estado brasileiro em robustas infraestruturas digitais públicas constitui fundamento de autonomia e controle efetivo de dados, não só para proteger interesses nacionais, mas para fortalecer a democracia e propiciar uma cultura de cidadania digital inclusiva. Dessa forma, o artigo pretende contribuir para o debate sobre soberania digital, democracia e cidadania inclusiva, destacando a importância da autonomia estatal, não só para

defesa dos interesses nacionais, mas também para proteção dos direitos fundamentais dos cidadãos no ciberespaço.

Inserido no campo da teoria crítica do direito e da governança digital, o presente estudo busca responder de que forma o colonialismo digital compromete a soberania estatal, a autonomia informacional e o exercício da cidadania democrática no Sul Global, especialmente no contexto brasileiro. Parte-se da hipótese de que a dependência tecnológica em relação às grandes plataformas transnacionais fragiliza a capacidade regulatória dos Estados e aprofunda assimetrias políticas, econômicas e comunicacionais, exigindo a construção de políticas públicas orientadas à soberania digital, à proteção de dados e à democratização do acesso às infraestruturas tecnológicas.

O estudo foi desenvolvido mediante abordagem qualitativa, de natureza teórico-dedutiva, utilizando técnica de revisão bibliográfica crítica. A investigação articula referenciais da teoria crítica, da governança digital e dos estudos decoloniais para examinar os impactos do colonialismo de dados sobre a soberania estatal e a cidadania democrática. O artigo estrutura-se em três eixos centrais: inicialmente, analisa-se a soberania digital e a tensão entre autonomia informacional e capitalismo de vigilância; em seguida, investigam-se as implicações da tecnologia para a democracia digital e para a formação de uma cidadania insurgente, a partir das contribuições de Donna Haraway, David Nemer e Deivison Faustino e Walter Lippold; por fim, refletem-se os desafios estratégicos da neutralidade de rede, do acesso à *internet* e da governança digital no contexto brasileiro.

2. SOBERANIA ESTATAL E COLONIALISMO DIGITAL: A TENSÃO ENTRE AUTONOMIA INFORMACIONAL E CAPITALISMO DE VIGILÂNCIA

Discutir soberania digital não é tarefa fácil. A teoria clássica da soberania teve em Jean Bodin seu ponto de partida e foi progressivamente desenvolvida por pensadores da modernidade, como John Locke, Jean-Jaques Rousseau, Thomas Jefferson, Alexander Hamilton, James Madison e John Jay. Ponto fundamental que surgiu em Bodin é compreender a soberania como poder absoluto e perpétuo, caracterizado pela ausência de qualquer autoridade superior (Scorsim, 2022).

Bonavides (2018, p. 219) destaca que a soberania, enquanto qualidade e fundamento do Estado-Nação, é expressão máxima de poder estatal e se apresenta em duas dimensões: a interna, em que a soberania explica o poder do Estado sobre o território e a população; dimensão externa, significando manifestação independente do poder de um Estado perante outros. Nesse

tópico, enfatizaremos a soberania na sua dimensão externa, relacionando-a ao colonialismo de dados e desafios à autonomia informacional do Estado brasileiro.

Com efeito, há soberania quando um ente político não está subordinado às ordens de outrem, exercendo autoridade suprema tanto no plano interno quanto externo: internamente, por meio da imposição legítima de normas e políticas públicas que organizam a vida em sociedade; externamente, pela independência frente a outros Estados. Esse status confere ao poder soberano a capacidade última de decisão e de autodeterminação, fundamentos essenciais para construção do Estado Democrático. No entanto, a Era Digital impõe desafios complexos à noção de soberania, fazendo com que se repense a teoria clássica.

O avanço do neoliberalismo impôs uma nova forma de difusão da informação: a internet tornou-se um fenômeno social pela facilidade de acesso, universalidade de estrutura, descentralização, velocidade de transmissão e dupla via em que a informação é transmitida. No ambiente digital, grandes empresas, como as *Big Techs*, operacionalizam estratégias de mercado por meio de plataformas que capturam informações pessoais de usuários e as utilizam para maximizar lucro.

A captura de dados, por si só, não é algo necessariamente ruim. Há situações em que pode ser necessária para viabilizar o funcionamento de plataformas, como no caso da utilização de dados de música para criar uma lista de músicas de acordo com o perfil do usuário. O problema está na falta de transparência, quando não se esclarece ao usuário como seus dados serão coletados e para que (ou para quem) serão compartilhados ou vendidos. Isso porque os dados revelam hábitos de pesquisa e moldam resultados de buscas de usuários, permitindo, a quem os coleta, controlá-los, modificá-los e até mesmo entregá-los a terceiros, à revelia de seus titulares.

Importa compreender que, no ambiente digital, tecnicamente, quando os dados são capturados em determinado território e submetidos a uma operação transfronteiriça de transferência ou compartilhamento para empresas sediadas em outro Estado, já se perde a soberania de origem. Uma vez coletados, os dados passam a estar sob a jurisdição do Estado onde se encontra a entidade receptora, ficando submetidos a uma nova estrutura de poder e controle voltada à satisfação dos interesses e necessidades desse país ou instituição (Pellegrini, 2023, p. 71). Dessa forma, a coleta massiva de informações se tornou a nova matéria-prima da economia informacional, fortemente explorada por setores de marketing e publicidade, consolidando um novo modelo de oferta de serviços e conteúdo, denominado *microtargeting*, o qual é personalizado de acordo com o perfil do usuário.

Tudo está a reforçar a assimetria de poder entre plataformas e Estados, demonstrando a capacidade daquelas de penetrarem em todos os aspectos da vida do cidadão e a fragilidade estatal de impor limites a esse avanço, dada a dependência tecnológica dos próprios Estados a empresas transnacionais. Explicita-se, assim, uma nova forma de dominação, de perpetuação da colonialidade sob vestes digitais, ultrapassando a dominação cultural, econômica e geográfica.

A respeito, Quijano (2005, p. 116) diferencia colonialismo de colonialidade: o primeiro consiste no processo de dominação direta e impositiva na perspectiva eurocêntrica; a colonialidade, por sua vez, diz respeito à continuidade da dominação. Segundo o autor, houve um processo de consolidação do conhecimento na perspectiva eurocêntrica – com a colonialidade – baseado no dualismo (europeu x não-europeu; civilizado x não-civilizado), de forma a evidenciar que tudo que não fosse europeu era considerado inferior. Historicamente, portanto, o colonialismo e, conseqüentemente, a colonialidade foram observados a partir da colonização europeia. Mas há três fases a destacar, segundo Cassino (2021, p. 31): a primeira se refere à colonização das Américas no século XVI, cujas independências foram alcançadas majoritariamente no século XIX; a segunda, trata da colonização da Ásia e África, cujas liberações se deram no pós-Segunda Guerra Mundial; por fim, a terceira fase diz respeito à expansão das tecnologias informacionais que origina o “colonialismo de dados”, também denominado “colonialismo digital” ou “neocolonialismo”.

No espaço digital, o colonialismo reproduz as práticas predatórias extrativistas associadas à quantificação massiva da vida social e à captura permanente de dados, aprofundando relações de dependência tecnológica e subordinação informacional. A colonialidade define um padrão de poder que subjuga o usuário (colonizado), anulando sua vontade, promovendo a invisibilidade de suas necessidades, compelindo-o a agir e pensar em benefício dos “setores de quantificação social” (colonizador) que são as corporações envolvidas em capturar o dia a dia dos usuários, responsáveis por capturar, quantificar e transformar os dados para posterior utilização econômica (Couldry; Mejías, 2018).

Cassino (2021, p. 13-31) destaca que, no colonialismo digital, nada deve ser excluído nem apagado, as pessoas e as coisas passam a fazer parte de infraestruturas de conexão informacionais, nas quais a captura em massa de dados passa a ser central. Na visão de Couldry e Mejías (2018), esses novos tipos de relações que permitem a extração de informações pessoais para exploração lucrativa, denomina-se *data relations*, algo como relações baseadas em dados.

Essa tensão entre dominação tecnológica e emancipação informacional é central em *Colonialismo Digital*: por uma crítica hacker-fanoniana, de Deivison Faustino e Walter Lippold

(2023). Em sua obra, os autores denunciam as formas contemporâneas de exploração e controle que caracterizam o colonialismo de dados. Para eles, o “novo colonialismo é datafocado” e sua violência se manifesta na precarização do trabalho, na vigilância algorítmica e na subordinação informacional dos países periféricos. Inspirados em Frantz Fanon, Faustino e Lippold afirmam que o colonialismo digital reproduz as hierarquias raciais e econômicas do passado sob a aparência de neutralidade tecnológica.

A denúncia formalizada por Faustino e Lippold (2023) evidencia o movimento expansionista liderado pelas *big techs* em áreas estratégicas de acesso e rastreamento de usuários. Com emprego de tecnologia de ponta, empresas transnacionais conseguem se inserir em todas as camadas do modelo de *cloud computing* – rede física, *Infrastructure as a Service* (IaaS), *Platform as a Service* (PaaS) e *Software as a Service* (SaaS). Em consequência, acabam por promover o abastecimento em maior ou menor escala de empresas privadas e dos próprios sistemas dos entes públicos. Ou seja, exercem domínio informacional por meio do controle de três camadas estruturantes da comunicação em rede, quais sejam: a) infraestrutura; b) protocolos de comunicação; c) plataformas de serviços e aplicações.

A partir dessa perspectiva, conclui-se que colonialismo digital opera em um sistema econômico que foi igualmente reconfigurado pelo avanço da tecnologia, ao qual Shoshana Zuboff (2019) denomina “capitalismo de vigilância”. Segundo a autora, nessa faceta o capitalismo utiliza o comportamento humano (não mais a mão-de-obra) como meio para captação de dados, produção de lucro e controle de mercado.

Zuboff (2019) demonstra que grandes corporações centralizam serviços digitais, monitoram usuários e processam dados em larga escala com o objetivo de consolidar hegemonia econômica e informacional. Essa dinâmica permite não apenas extrair e mercantilizar comportamentos, mas também produzir mercados, antecipar tendências e influenciar decisões individuais e coletivas por meio da predição algorítmica. Empresas como Google, Amazon, Meta e Microsoft passaram, assim, a exercer poder que transcende o domínio econômico, alcançando dimensões políticas, culturais e comunicacionais.

Os dados transformaram-se em commodities estratégicas da economia digital. Segundo Silveira (2017), a modulação do comportamento humano constitui o principal objetivo do mercado de dados, especialmente por meio de mecanismos capazes de atuar sobre a atenção, a memória e a subjetividade dos usuários. Os dispositivos digitais tornam-se particularmente eficazes quando articulados à emoção e ao comportamento cotidiano, permitindo a criação de ambientes informacionais direcionados à influência permanente do indivíduo.

Assim, as técnicas de modulação não são simplesmente a difusão de notícias e publicidade, mas a criação de “situações sociais”. Até o plano de fundo social passa a ser justificativa para captação de dados, pois ao disponibilizar conectividade às pessoas que não dispõem de recursos financeiros para acessar a rede, a entrega de dados passa a ser moeda de troca, possibilitando uma análise comportamental do usuário para, então, direcionar conteúdo, como fonte lucrativa. É dessa forma que o poder econômico se torna difuso e, não raras vezes, o das *big techs* é superior ao dos Estados-Nação.

Essa lógica, porém, é difícil de ser detectada, porque se baseia em uma assimetria de conhecimento, de forma que o usuário, na maioria das vezes, sequer percebe o que está acontecendo. Assim, de maneira imperceptível, o usuário fornece seus dados, seja para antecipar o que deseja seja para obter informações de forma rápida e simples; mas o faz sem saber o que será feito com os dados coletados. Não há, portanto, voluntariedade na conduta à medida em que o usuário não reúne informações claras, objetivas e suficientes sobre as consequências do fornecimento de seus dados, o que se agrava à medida em que o Estado não consegue proteger seus cidadãos.

Nesse escopo, Sérgio Amadeu da Silveira e Jeff Xiong (2025) definem a soberania digital como a capacidade de uma sociedade e de um Estado de controlar e governar tecnologias essenciais para autodeterminação, proteção de direitos e desenvolvimento. No artigo, publicado na Liinc em Revista, os autores contextualizam esse conceito como uma reação ao colonialismo digital, caracterizado pela dependência tecnológica de países do Sul Global em relação às grandes potências e corporações, especialmente dos Estados Unidos.

Sob essa perspectiva, a captura massiva de dados ameaça a própria democracia ao possibilitar a criação de perfis detalhados dos eleitores. A cidadania, expressa no ato de votar, pressupõe que o eleitor tenha consciência crítica sobre as propostas de governo apresentadas; contudo, essa consciência é comprometida quando candidatos utilizam dados pessoais de forma oculta para identificar expectativas individuais e moldar suas campanhas em função delas. Trata-se de uma manipulação informacional que distorce o debate público e fragiliza a autonomia política do cidadão.

No mundo digital, em que o domínio informacional dita o ritmo das relações, impõe-se a urgência de controle efetivo dos dados – tanto por meio da regulação do ciberespaço quanto pela garantia do exercício de direitos fundamentais. Por esse viés, a compreensão clássica de soberania já não mais se sustenta nos tempos atuais; sua definição transcende a mera capacidade normativa do Estado, envolve o controle efetivo sobre protocolos, linguagens, data centers, tráfego de dados, computação em nuvem e infraestrutura física e lógica da *internet*. Em outras

palavras, soberania, em tempos digitais, diz respeito, não só aos aspectos de autoridade e direito, mas principalmente à autonomia informacional e capacidade de controle de dados, informações e conteúdos digitais. Na visão de Pellegrini (2023, p. 71), a soberania digital traduz a autoridade de um Estado e de sua sociedade em controlar aspectos da “criatividade e inventividade” e de seus dados.

No Brasil, a soberania digital constitui fundamento do próprio Estado de Direito, traduzido como instrumento de proteção de interesses nacionais. Apesar disso, Silveira e Xiong (2025) alertam para o baixo nível de soberania digital do país, de acordo com o Índice de Soberania Digital, por eles proposto, que evidencia a fragilidade brasileira nesse campo. Esse índice foi construído a partir de quatro critérios - dados, infraestrutura digital, governança digital e capacidade digital -, que medem o grau de independência tecnológica de um país. Os critérios abrangem desde a proteção, armazenamento e propriedade dos dados, passando pelo domínio sobre hardware, software e redes de comunicação, até a autonomia legislativa e de pesquisa e desenvolvimento. O Brasil foi classificado em níveis baixos porque, embora possua marcos normativos relevantes como o Marco Civil da *Internet* e a Lei Geral de Proteção de Dados (LGPD), mantém forte dependência de plataformas e infraestruturas estrangeiras, carece de políticas industriais de tecnologia e apresenta baixo investimento em inovação e formação de capacidades digitais próprias, o que compromete sua autodeterminação no ambiente digital.

Esse alerta de Silveira e Xiong (2025) condiz com o atual cenário brasileiro, dadas as inúmeras tentativas do Estado brasileiro de construir formas de interlocução institucional com plataformas digitais, sem qualquer efetividade, como evidenciam episódios envolvendo bloqueios unilaterais de conteúdo, resistência à regulação normativa ou mesmo a judicialização de temas sensíveis. Para avançar nesse campo, os autores sinalizam a necessidade de fortalecer a formação em ciência, tecnologia, engenharia e matemática, ampliar investimentos em infraestrutura digital pública, retomar a coordenação estatal na produção tecnológica nacional e estabelecer cooperação internacional estratégica, especialmente com países do Sul Global, a fim de reduzir a dependência tecnológica dos Estados Unidos.

Em síntese, na Era digital, a soberania depende da autonomia regulatória, do controle soberano sobre o fluxo de dados e da existência de infraestruturas digitais públicas livres da subordinação a corporações estrangeiras e à lógica hegemônica da ordem digital transnacional. Embora a cooperação internacional seja relevante, ela não pode se converter em dependência estatal diante de agentes e setores estratégicos. Diante desses desafios, a soberania digital configura-se como tema de segurança nacional, abrangendo a autonomia informacional, a capacidade regulatória sobre o ciberespaço e a garantia do exercício dos direitos fundamentais

no ambiente digital. Impõe-se ao Estado brasileiro superar toda forma de dependência informacional, condição indispensável à defesa de interesses nacionais e à autodeterminação dos povos. Em uma realidade marcada pela centralização privada da infraestrutura tecnológica e pela mercantilização dos dados, a soberania digital deixa de constituir mera pauta regulatória e passa a representar condição de preservação da democracia, da autodeterminação dos povos e da efetividade dos direitos fundamentais. Sem autonomia tecnológica, capacidade regulatória e controle estratégico das infraestruturas digitais, o Estado torna-se progressivamente incapaz de proteger seus cidadãos das novas formas de colonialidade informacional que estruturam o capitalismo contemporâneo.

3. DEMOCRACIA DIGITAL E CIDADANIA INSURGENTE: A *INTERNET* COMO INSTRUMENTO POLÍTICO DE EMANCIPAÇÃO NA PERSPECTIVA DE HARAWAY, NEMER, FAUSTINO e LIPPOLD

A construção contemporânea da democracia e da cidadania desloca-se progressivamente para o campo digital, onde o acesso à *internet* emerge como direito fundamental e instrumento de inclusão social. A virtualização afeta não apenas a informação e a comunicação, mas também os corpos, o desenvolvimento da economia e marcos coletivos de vínculos sociais. Neste tópico, analisaremos as reflexões de Donna Haraway, David Nemer, Deivison Faustino e Walter Lippold sobre o fenômeno digital, cujos ensinamentos articulam crítica social, emancipação tecnológica e insurgência política em torno de um mesmo eixo: o uso da tecnologia como meio de ampliação da democracia e de reinvenção da cidadania.

Em primeiro plano, destaca-se que, no espaço digital, todos são parte da universalização do sujeito, ou seja, o “eu” se apresenta despersonalizado e se reconfigura através da afinidade de interesses que são partilhados entre pluralidades, sejam de pessoas sejam de coletivos, com existência física ou virtual. Nessa dimensão, o “eu virtual” integra-se ao “eu real” de forma a não ser mais possível dissociar a tecnologia do sujeito (Lévy, 2010). Com esse olhar, Donna Haraway (2009, p. 36-99) propõe, em *Antropologia do Ciborgue*, no célebre Manifesto Ciborgue, uma metáfora política e filosófica que redefine as fronteiras entre o humano e o tecnológico.

O ciborgue, “um híbrido de máquina e organismo, uma criatura de realidade social e também de ficção”, representa, para a autora, a possibilidade de subverter as oposições tradicionais que sustentaram o pensamento moderno - natureza e cultura, corpo e mente, homem e mulher, centro e periferia. Haraway defende que a libertação passa pela “construção da

consciência da opressão e da apreensão da possibilidade”, isto é, pela capacidade de reconhecer que a tecnologia não é neutra, mas pode ser reapropriada como ferramenta de transformação social e política. Ao afirmar que “prefere ser uma ciborgue a ser uma deusa”, Haraway rompe com as visões nostálgicas que idealizam um retorno a uma natureza perdida e propõe uma nova ontologia política, em que a cidadania se constrói na mistura, na interconexão e na pluralidade. Nesse sentido, o ciborgue torna-se um símbolo da cidadania insurgente contemporânea - híbrida, crítica e consciente das contradições que atravessam a tecnocultura.

Essa dimensão emancipadora da tecnologia é também o ponto de partida de Tecnologia do Oprimido, de David Nemer (2021), cuja obra desloca o olhar da teoria para a prática cotidiana das comunidades periféricas brasileiras. A partir de uma etnografia digital em favelas, Nemer demonstra como moradores de territórios marginalizados se apropriam de tecnologias mundanas - como celulares, *lan houses* e telecentros - para resistir à exclusão e criar formas próprias de participação social. Inspirado em Paulo Freire, o autor compreende a tecnologia como um meio de libertação: “apropriar-se das tecnologias mundanas é o ato de esperança; eles usam a tecnologia para buscar a libertação”.

Essa apropriação insurgente revela que a inclusão digital vai muito além do acesso técnico à rede, abrange a criação de espaços de convivência, reconhecimento e solidariedade. Os telecentros, segundo Nemer, não são apenas instrumentos de capacitação profissional, mas lugares onde “conhecidos se transformam em pessoas mais próximas, e onde participavam de territórios informativos”, revelando o potencial político da sociabilidade mediada pela *internet*. O autor ressalta que, no Brasil, o Marco Civil da *Internet* (Lei nº 12.965/2014) reconhece o acesso à rede como um direito fundamental, equiparando-o à educação e à saúde; nesse sentido, as plataformas podem ser compreendidas como arenas de sobrevivência política, através das quais o oprimido denuncia violências, preserva vínculos familiares e afirma sua identidade.

Faustino e Lippold (2023) convergem com a ideia de Nemer e defendem uma crítica “hacker-fanoniana”, na qual os sujeitos periféricos assumem o protagonismo da descolonização tecnológica. Para os autores, a resistência nasce nas bordas do sistema – nas periferias, clubes de ciência populares, coletivos de programadores e redes cooperativas de plataforma - que encarnam a luta por emancipação digital. Segundo Faustino e Lippold, “a descolonização da tecnologia passa pela compreensão, pela ação e pelo controle dos meios tecnológicos por parte dos trabalhadores da periferia do capitalismo”. Assim sendo, a tecnologia deixa de ser apenas território do político – onde se disputa quem conta, quem calcula e quem conecta; mas, passa a constituir território de libertação. Os autores apontam para a urgência de descolonizar a tecnologia, ou seja, deslocar o eixo de poder, através de técnicas insurgentes, antirracistas e

tecnopolíticas, de maneira a reconhecer que o conhecimento não é neutro e a infraestrutura não é inocente. Nessa direção, segundo eles, será possível reapropriar o saber e hackear a tecnologia, através do uso criativo e coletivo das redes.

Sintetizando, Haraway, Nemer, Faustino e Lippold reconhecem a tecnologia como campo de disputa política e ontológica, admitindo que possa ser instrumentalizada para fins de dominação ou de libertação. Para Haraway, o ciborgue é a metáfora da resistência híbrida que se recusa a aceitar fronteiras impostas; para Nemer, as práticas digitais nas favelas são formas concretas de insurgência e de reconstrução da cidadania; para Faustino e Lippold, a luta pela emancipação digital é a continuação da luta anticolonial, agora travada nas redes informacionais. Ambos reconhecem que o acesso à *internet* não é apenas uma questão técnica, mas um ato político - um direito à fala, à presença e à produção de sentido no espaço público global.

A partir dessas leituras, torna-se evidente que a democracia digital ultrapassa a simples ampliação do acesso às tecnologias, pois envolve garantir condições efetivas para que sujeitos historicamente silenciados possam agir, narrar e decidir sobre o próprio futuro. A democracia, nesse contexto, é responsável por promover uma cultura de cidadania, esta última compreendida como condição que habilita o indivíduo a participar da vida pública e não se reduz ao direito de votar (Silva, 1992, p. 305). Sob essa perspectiva, o ambiente digital emerge como novo espaço de disputa, no qual se manifestam tanto potencialidades de inclusão quanto barreiras invisíveis de exclusão algorítmica que desafiam a concretização de uma cidadania plenamente democrática.

Segundo Nemer (2021), exclusão digital não se limita à ausência de infraestrutura tecnológica. Ela também se manifesta por mecanismos silenciosos de invisibilização algorítmica, mediante plataformas que priorizam conteúdos alinhados a padrões econômicos, culturais e políticos hegemônicos. Nesse contexto, determinadas identidades, narrativas e formas de existência tornam-se menos visíveis, menos circuláveis e menos reconhecidas no ambiente digital, reproduzindo desigualdades históricas sob novas formas tecnológicas.

A sistemática do silenciamento opera por omissão, não por censura explícita: é a ausência no buscador, o sumiço do *feed*, a exclusão disfarçada de “adequação a padrões”, dificuldade de viralização de conteúdo de denúncia e afirmação identitária, como alerta Virginia Eubanks (2017). Por conseguinte, a *internet* transforma-se em território de insurgência que, por sua vez, assume múltiplas formas: criação de páginas comunitárias, perfis coletivos em redes sociais, campanhas de mobilização, produção de vídeos e *podcasts*, participação em fóruns digitais e construção de redes comunitárias.

Ao partilhar visões de mundo e experiências de luta nas redes, indivíduos marginalizados questionam o que é considerado “visível”, “digno de ser viralizado” ou “adequado” à cultura digital. O *like* transforma-se em um ato de insurgência: um grito público de existência que desafia o silêncio das redes: Quem tem o direito de ser visto? Quem conquista o direito de existir no mundo digital?

Cada prática de apropriação coletiva da tecnologia (seja por redes comunitárias, iniciativas *hacker*, plataformas cooperativas ou produção autônoma de conteúdo) representa forma contemporânea de resistência ao colonialismo digital. Essas experiências demonstram que a cidadania digital não se resume ao acesso técnico à *internet*, mas envolve a possibilidade concreta de participação, reconhecimento e produção de sentidos no espaço público global. Como defendem Faustino e Lippold (2023), “a chance de descolonização tecnológica é a criação ou o fortalecimento de novas formas de luta e organização”. Não ser deletado, nesse contexto, converte-se em ato político de resistência, por meio do qual a cidadania insurgente se afirma no espaço digital, democratizado na luta pela emancipação, na qual o humano e o tecnológico se unem, não para reforçar a dominação, mas enfrentar o colonialismo de dados.

4. A NEUTRALIDADE DE REDE E O ACESSO À INTERNET: DESAFIOS ESTRATÉGICOS DO ESTADO BRASILEIRO À GOVERNANÇA DIGITAL

Como visto, a insurgência cidadã impõe ao Estado brasileiro o dever de adotar uma postura ativa de enfrentamento ao colonialismo digital, com políticas que garantam não apenas o acesso universal e a neutralidade da rede, mas assegurem condições para o exercício da cidadania. Trata-se de obrigação que decorre da centralidade das práticas digitais na vida contemporânea; afinal, torna-se legítimo questionar até que ponto o indivíduo pode, por si só, suprir suas necessidades básicas ou se depende, necessariamente, da ação estatal para concretizá-las no ambiente digital. Neste tópico, analisaremos a neutralidade de rede como núcleo do direito fundamental à *internet* e os desafios estratégicos do Estado para implemento da governança digital e proteção de dados dos usuários.

De início, registramos que o século XXI foi marcado pelo avanço da tecnologia, a qual conduziu à reestruturação da morfologia social. Não se pode mais dissociar a relação entre tecnologia e sociedade, dada a reconfiguração dos mais variados aspectos da vida humana, sociais, econômicos, financeiros e produtivos. Isso fez com que a sociedade se organizasse em redes digitais e passasse a se conectar por tecnologias cibernéticas que emergem em plataformas

diversas de relacionamento on-line, com implicações à percepção de espaço público e à própria atuação estatal.

O acesso à *internet* deixou de ser um privilégio tecnológico e passou a ser reconhecido como um direito fundamental, diretamente vinculado à dignidade humana e à inclusão social. Essa transformação impõe ao Estado brasileiro a responsabilidade urgente de regulamentar seu uso e garantir sua universalização, especialmente diante dos riscos que o ambiente digital apresenta aos usuários - da captura indevida de dados à violação da privacidade e da liberdade individual.

Note-se, com isso, que a proteção de dados pessoais está atrelada ao direito à *internet*, apresentando-se como dever, tanto do setor público quanto do privado, seguir regras rígidas para coletar, processar, compartilhar e resguardar informações pessoais, esclarecendo o usuário sobre quais dados serão coletados, para quais finalidades serão utilizados e, principalmente, municiando-o de ferramentas que possibilitem a exclusão das informações já coletadas ou interrupção da coleta. Nesse concernente, declaram Sousa, Cristóvam e Machado (2022, p. 184):

A regulação de grandes atores privados do setor de tecnologia consiste na determinação do complexo de ações e técnicas aplicáveis nesse espaço, a prevenir e corrigir práticas que violem aspectos nucleares da dignidade humana, os direitos fundamentais e o próprio funcionamento equilibrado da configuração de Estado.

O Brasil reconheceu formalmente o acesso à *internet* como direito fundamental através da promulgação da Lei nº 12.965/2014, denominada Marco Civil da Internet. Nessa legislação são estabelecidos princípios, garantias, direitos e deveres para o uso da rede. O artigo 7º assegura aos usuários “o acesso à internet essencial ao exercício da cidadania”, situando a conectividade como condição indispensável para o gozo de outros direitos constitucionais, como a liberdade de expressão, o direito à informação e a igualdade de oportunidades. E, um dos pilares que sustentam esse direito é o princípio da neutralidade da rede, também previsto no Marco Civil da Internet, no artigo 9º. Esse dispositivo impede que provedores e operadoras de telecomunicações discriminem ou priorizem conteúdos, aplicações ou serviços, assegurando que todos os usuários tenham acesso igualitário às informações disponíveis.

A neutralidade significa que todo o tráfego de dados deve ser tratado de forma isonômica, sem distinção por conteúdo, origem, destino, serviço, terminal ou aplicação. Dito de outra forma, proíbe-se que provedores ou operadoras privilegiem determinados sites, plataformas ou usuários em detrimento de outros. Essa diretriz preserva a internet como espaço

democrático e plural, impedindo que interesses econômicos ou políticos limitem o acesso à informação ou estabeleçam hierarquias entre cidadãos. A neutralidade da rede é, portanto, o núcleo do direito fundamental à internet, apresentando a natureza livre e aberta como condição indispensável para inclusão e participação social, ou seja, ao exercício pleno da cidadania.

Por sua vez, através da Lei nº 13.079/2018, denominada Lei Geral de Proteção de Dados, o Estado brasileiro avançou no equilíbrio entre desenvolvimento tecnológico/ inovação e proteção à autodeterminação informativa, à liberdade de expressão, ao direito à informação. Tais legislações resultam do desdobramento contemporâneo de direitos fundamentais previstos na Constituição de 1988, especialmente do artigo 5º, que protege a liberdade e a privacidade, e do artigo 3º, que define como objetivo de a República construir uma sociedade livre, justa e solidária, promovendo o bem de todos, sem discriminação.

Diante disso, o Estado brasileiro possui o dever constitucional de implementar medidas que assegurem condições a todos, sem discriminação, de acesso universal, igualitário e de qualidade à internet, protegendo dados pessoais de seus usuários, como parte de sua função de concretizar direitos fundamentais e reduzir desigualdades. A obrigação, enfatize-se, decorre não apenas do Marco Civil, mas também dos princípios constitucionais da igualdade, da universalização dos serviços públicos e da promoção do desenvolvimento nacional. O acesso à internet deve ser entendido como serviço essencial, assim como a educação, a saúde e a moradia. Cabe ao poder público formular políticas públicas que ampliem a infraestrutura digital, especialmente nas regiões periféricas, rurais e em comunidades tradicionalmente excluídas, assegurando que o direito à conexão seja efetivo e não meramente formal, com proteção de dados.

Com efeito, em uma sociedade cada vez mais estruturada sobre fluxos informacionais, a capacidade do Estado de gerir, regular e universalizar o ambiente digital tornou-se imprescindível ao exercício da cidadania e fortalecimento da democracia. Nesse cenário, a governança digital apresenta-se como eixo estratégico para o fortalecimento da democracia e a proteção da autonomia informacional, pois articula políticas públicas, mecanismos regulatórios e infraestruturas tecnológicas voltadas à preservação do interesse nacional no ciberespaço. À luz da crescente disputa geopolítica por controle das infraestruturas digitais - como evidenciado na competição sino-americana pelo domínio das redes 5G, a governança digital representa o instrumento por meio do qual o Estado brasileiro busca assegurar o direito fundamental de acesso à internet, a neutralidade de rede e a proteção de dados pessoais, coibindo monopólios tecnológicos e assegurando transparência algorítmica e regulatória (Maria et al., 2025).

Entendida como o conjunto de políticas, normas, processos e tecnologias voltados à gestão dos recursos digitais e à promoção de um ambiente informacional seguro, interoperável e inclusivo, a governança digital deve ser guiada por princípios de transparência, participação social, soberania e justiça digital. Seu objetivo é garantir que o espaço virtual não se converta em território de dominação econômica ou política - risco acentuado pela concentração de poder nas plataformas estadunidenses e pelo avanço das infraestruturas tecnológicas chinesas -, mas em um ecossistema plural e equitativo, coerente com os valores constitucionais da dignidade humana e da igualdade (Scorsim, 2022; Fefèvre, 2024).

Por meio de uma política sólida de governança digital, o Estado brasileiro assume o dever de fomentar o letramento digital e a inclusão tecnológica como instrumentos de redução das desigualdades sociais e regionais, conforme previsto no artigo 3º, inciso IV, da Constituição Federal de 1988. Isso implica reconhecer que essa governança transcende a gestão técnica das redes: trata-se de uma função pública essencial, comprometida com a democratização do acesso, a equidade e a efetivação dos direitos fundamentais no ambiente virtual. Em consonância com o que apontam Maria et al. (2025), tal governança deve também fortalecer a autonomia tecnológica nacional, incentivando a produção endógena de inovações e a cooperação entre universidades, empresas e Estado, para que o Brasil não permaneça refém de sistemas e plataformas estrangeiras.

A materialização dessa forma de governança pode ser observada em iniciativas estatais de digitalização de serviços e de aproximação entre governo e sociedade. O desenvolvimento do Governo Eletrônico (e-Gov) exemplifica a aplicação de recursos tecnológicos que ampliam a eficiência administrativa e a transparência, reconfigurando o Estado como canal democrático e de inclusão digital. Contudo, como destaca o debate contemporâneo sobre soberania digital, essa virtualização também exige mecanismos de *accountability* algorítmica e de gestão ética dos dados, sob pena de o poder público reproduzir práticas opacas semelhantes às das corporações privadas. Assim, o desafio do Estado não se limita à prestação eficiente de serviços digitais, mas se estende ao dever de garantir a confiança cívica e o controle social sobre os fluxos informacionais que sustentam a vida pública digital (Grohmann; Barbosa, 2025).

Nessa linha de raciocínio, a governança digital se conecta diretamente ao investimento em Infraestruturas Públicas Digitais (IPDs) - redes, plataformas e sistemas sob domínio estatal - capazes de assegurar autonomia informacional, soberania tecnológica e proteção estratégica dos dados nacionais. Conforme ressaltam Maria et al. (2025), a dependência de infraestruturas estrangeiras e de provedores privados representa risco à autodeterminação digital e ao desenvolvimento soberano do país. As IPDs, portanto, constituem não apenas instrumentos de

prestação de serviços públicos, mas ativos estratégicos de defesa e desenvolvimento, essenciais ao enfrentamento do colonialismo tecnológico e à consolidação de um Estado digital autônomo e inclusivo.

O investimento em IPDs e em políticas de governança digital deve ser reconhecido como objetivo fundamental da República Federativa do Brasil, indispensável ao desenvolvimento nacional e à construção de uma sociedade livre, justa e solidária, como estabelece o art. 3º da Constituição de 1988. Implica reconhecer na infraestrutura digital o mesmo valor público atribuído, historicamente, às políticas de saúde, educação e transporte, reconhecendo a conectividade e a soberania informacional como dimensões da cidadania.

Nessa perspectiva, o Estado brasileiro reafirma seu papel como garantidor de direitos na Era da Informação, assumindo o dever de proteger dados pessoais, combater a exploração e a manipulação algorítmica e assegurar a neutralidade da rede como fundamento da liberdade de expressão. Cabe-lhe, ainda, instituir mecanismos de governança digital democrática e multissetorial sobre as infraestruturas tecnológicas. Nesse contexto, o conceito de governança transcende a dimensão administrativa e se consolida como expressão contemporânea do Estado Democrático de Direito - um modelo de gestão comprometido com a inclusão digital, a transparência e a efetividade dos direitos fundamentais em um mundo cada vez mais mediado por dados e tecnologias.

5. CONSIDERAÇÕES FINAIS

A análise conjunta das três dimensões abordadas - soberania digital, cidadania insurgente e governança em rede - permite compreender que a consolidação de um Estado democrático na Era da informação requer a articulação entre autonomia tecnológica, inclusão digital e proteção de direitos fundamentais. O debate sobre a soberania frente ao colonialismo de dados evidencia que o poder contemporâneo não se exerce apenas sobre territórios, mas sobre fluxos informacionais. A dependência tecnológica e a captura transnacional de dados instauram novas formas de dominação e reiteram antigas hierarquias coloniais sob roupagem digital. Romper com essa lógica implica reconhecer a autonomia informacional como dimensão estratégica da soberania nacional, assegurando ao Estado-Nação o controle efetivo sobre infraestrutura digital e capacidade de regular as plataformas que operam em seu território.

No cenário brasileiro, a democracia digital revela-se como o espaço de resistência e reconfiguração da cidadania. As reflexões de Haraway, Nemer, Faustino e Lippold demonstram que o ambiente digital, embora permeado por estruturas de vigilância e exclusão, pode ser

apropriado como território de libertação. Nesse contexto, a cidadania deixa de ser uma categoria estática e se transforma em prática viva de enfrentamento das desigualdades, expressada em ações de coletivos, movimentos e sujeitos que reivindicam visibilidade e voz nas redes. A insurgência digital não se limita à crítica do poder tecnológico, mas à sua reconfiguração a partir da criatividade e da resistência popular, instrumentalizando a internet em político de emancipação e afirmação de identidades.

A governança digital constitui o elo de coesão entre soberania e cidadania no ciberespaço. Dessa forma, o Estado assume o dever do Estado de estabelecer mecanismos institucionais que assegurem o acesso universal e a neutralidade da rede, promovendo letramento digital e ampliando infraestruturas públicas capazes de garantir autonomia informacional. A implementação de políticas de governança orientadas pela transparência, pela inclusão e pela equidade constitui o caminho para que a tecnologia efetivamente seja utilizada em prol do interesse público, e não do interesse neoliberal de controle e lucro.

De forma geral, investir em Infraestruturas Públicas Digitais (IPDs) é investir na própria democracia: significa fortalecer a soberania nacional, reduzir desigualdades regionais e assegurar que o espaço digital se mantenha livre, seguro e plural. A eficácia do direito fundamental à internet pressupõe garantir a neutralidade de rede, com implicações à cidadania. O desafio brasileiro está em conjugar soberania, cidadania e governança digital de forma plural e indissociável. Isso porque a cidadania constitui força motriz para democratização das redes; enquanto a governança, o instrumento capaz de equilibrar ambas, com transparência e segurança digital.

REFERÊNCIAS BIBLIOGRÁFICAS

BONAVIDES, Paulo. *Curso de Direito Constitucional*. 25 ed. São Paulo: Malheiros, 2018.

CASSINO, João Francisco. O Sul Global e os desafios pós-coloniais na era digital. In: SILVEIRA, Sérgio Amadeu da; SOUZA, Joyce; CASSINO, João Francisco (org.). *Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal*. São Paulo: Autonomia Literária, 2021, p. 13-31.

COULDRY, Nick; MEJÍAS, Ulises A. *Data colonialism: rethinking big data's relation to the contemporary subject*. *Television e New Media*, v. 20, n. 4, p. 336-349, 2019.

EUBANKS, Virginia. *Automating inequality: how high-tech tools profile, police, and punish the poor*. Nova Iorque: St. Martin's Press, 2017.

FAUSTINO, Deivison; LIPPOLD, Walter. *Colonialismo digital: Por uma crítica hacker-fanoniana*. São Paulo: Boitempo, 2023.

GROHMANN, Rafael; BARBOSA, Alexandre Costa. *Big tech sovereignty: platforms and discourse of sovereignty-as-a-service*. AoIR Selected Papers of Internet Research, 2025. Disponível em: <https://spir.aoir.org/ojs/index.php/spir/article/view/13948>. Acesso em: 29/10/2025.

HARAWAY, Donna. Manifesto ciborgue: ciência, tecnologia e feminismo-socialista no final do século XX. In: HARAWAY, Donna; KUNZRU, Hari; TADEU, Tomaz (Orgs.). *Antropologia do ciborgue: as vertigens do pós-humano*. Belo Horizonte: Autêntica Editora, 2009.

LEFÈVRE, Flávia. *Soberania digital - aspectos legais e políticos*. Blog da Flávia Lefèvre, 22 jun. 2024. Disponível em: <https://flavialefevre.com.br/pt/soberania-aspectos-legais-e-politicos>. Acesso em: 29/10/2025.

LÉVY, Pierre. *Cibercultura*. São Paulo: Editora 34, 2010.

MARIA, Isadora de Moraes; DIAS, Rafael de Brito; PERÓN, Alcides Eduardo dos Reis; GIBERTINI, Pietro. *A disputa sino-americana pelas infraestruturas digitais de 5G e seus reflexos sobre a soberania digital no Brasil*. Liinc em Revista. Rio de Janeiro, v. 21, n. 1, e7541, 2025. Disponível em: <https://revista.ibict.br/liinc/article/view/7541>. Acesso em: 29/10/2025.

NEMER, David. *Tecnologia do Oprimido: desigualdade e o mundano digital nas favelas do Brasil*. Vitória: Editora Milfontes, 2021.

PELLEGRINI, Jerônimo *et al.* Inteligência local, soberania digital e soberania de dados. In: PENTEADO, Cláudio; PELLEGRINI, Jerônimo; SILVEIRA, Sérgio Amadeu da (Orgs.). *Plataformização, inteligência artificial e soberania de dados: tecnologia do Brasil 2020-2030*. São Paulo: Ação Educativa, 2023. Disponível em: https://acaoeducativa.org.br/wp-content/uploads/2024/01/tecnologia_no_brasil_2020_2030.pdf. Acesso em: 26/10/2025.

QUIJANO, Aníbal. Colonialidade do poder, eurocentrismo e América Latina. In: LANDER, Edgardo (Org.). *A colonialidade do saber: eurocentrismo e ciências sociais: perspectivas latino-americanas*. Buenos Aires: CLACSO, 2005. Disponível em: https://biblioteca.clacso.edu.ar/clacso/sur-sur/20100624103322/12_Quijano.pdf. Acesso: 08/09/2025.

SCORSIM, Edison. *Soberania digital, dados, cibernética e tecnologia: conectividade, as redes de telecomunicações 5G, computação em nuvem, entre outros temas relevantes*. In: CLÈVE, Clèmerson Merlin (Org.). *Direito constitucional brasileiro: constituições econômica e social*. São Paulo: Editora Revista dos Tribunais, 2022.

SILVEIRA, Sérgio Amadeu da. *Tudo sobre tod@s*. Redes Digitais, privacidade e venda de dados pessoais. São Paulo: Edições Sesc, 2017.

SILVEIRA, Sérgio Amadeu da; XIONG, Jeff. *Índice de soberania digital: o caso do Brasil*. Liinc em Revista. Rio de Janeiro, v. 21, n. 1, e7451, jun. 2025. Disponível em: <https://revista.ibict.br/liinc/article/view/7451>. Acesso: 28/10/2025.

SOUSA, Thanderson; CRISTÓVAM, José Sérgio da Silva; MACHADO, Raquel Cavalcanti Ramos. Constitucionalismo e administração pública digitais: inovação tecnológica e políticas públicas para o desenvolvimento do Brasil. *Revista Brasileira de Políticas Públicas*, Brasília, v. 12, nº 2, p. 179-196, set. 2022.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power*. Nova Iorque: Public Affairs, 2019.