

UNIVERSIDADE FEDERAL DE OURO PRETO
DEPARTAMENTO DE DIREITO

ARTHUR LAGE GARCIA CARVALHO

**COLONIALISMO DE DADOS, SOBERANIA DIGITAL E OS LIMITES DA LGPD
NO BRASIL**

OURO PRETO
2026

ARTHUR LAGE GARCIA CARVALHO

**COLONIALISMO DE DADOS, SOBERANIA DIGITAL E OS LIMITES DA LGPD
NO BRASIL**

Trabalho de Conclusão de Curso apresentado ao
Departamento de Direito da Universidade Federal
de Ouro Preto, como requisito parcial para
obtenção do título de Bacharel em Direito.

Orientadora: Juliana Evangelista de Almeida

OURO PRETO

2026



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
ESCOLA DE DIREITO, TURISMO E MUSEOLOGIA
DEPARTAMENTO DE DIREITO



FOLHA DE APROVAÇÃO

Arthur Lage Garcia Carvalho

Colonialismo de dados, soberania digital e os limites da LGPD no Brasil

Monografia apresentada ao Curso de Direito da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de Bacharel

Aprovada em 14 de julho de 2026

Membros da banca

Doutora- Juliana Evangelista de Almeida- Orientador(a) Universidade Federal de Ouro Preto
Doutora- Andressa de Bittencourt Siqueira da Silva - Universidade Federal de Ouro Preto
Especialista- Elísio Hermenegildo da Silva Júnior - Universidade Federal de Ouro Preto

[Juliana Evangelista de Almeida, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 14/07/2026



Documento assinado eletronicamente por **Juliana Evangelista de Almeida, PROFESSOR DE MAGISTERIO SUPERIOR**, em 28/07/2026, às 09:45, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **1148240** e o código CRC **A5BC2D1B**.

RESUMO

A presente pesquisa analisa os limites da Lei Geral de Proteção de Dados Pessoais no enfrentamento da colonialidade de dados no Brasil, especialmente diante da atuação das grandes plataformas digitais transnacionais e da dependência brasileira em relação a infraestruturas tecnológicas estrangeiras. Parte-se da hipótese de que a LGPD, embora represente avanço normativo relevante na proteção dos titulares, não é suficiente, por si só, para conter práticas extrativistas baseadas na coleta, no processamento e na monetização massiva de dados pessoais. Para desenvolver essa análise, adota-se abordagem qualitativa, com revisão bibliográfica interdisciplinar e análise normativa da legislação brasileira, em diálogo com autores que discutem imperialismo, capitalismo de vigilância, colonialismo de dados, colonialidade do poder, epistemicídio e soberania digital. O trabalho examina, inicialmente, a concentração econômica e material das infraestruturas digitais, demonstrando que a chamada “nuvem” depende de cabos submarinos, data centers, servidores, energia, recursos naturais e regimes privados de propriedade. Em seguida, analisa os limites da LGPD quanto ao consentimento, à autodeterminação informacional, à atuação da ANPD, aos fluxos transfronteiriços de dados e à dependência de plataformas estrangeiras em setores estratégicos, como educação, saúde, Judiciário e administração pública. Por fim, discute alternativas para a construção de uma soberania digital democrática no Brasil, a partir do diálogo com referências regulatórias internacionais, especialmente o GDPR e a PIPL, da crítica hacker-fanoniana e de propostas voltadas ao fortalecimento da infraestrutura pública, da transparência algorítmica, da contratação pública estratégica e da educação digital crítica. Conclui-se que a LGPD é necessária, mas insuficiente para enfrentar a colonialidade de dados, sendo indispensável articulá-la a um projeto mais amplo de autonomia tecnológica, controle social e soberania digital.

Palavras-chave: colonialismo de dados; soberania digital; LGPD; Big Techs; proteção de dados pessoais.

ABSTRACT

This research analyzes the limits of the Brazilian General Personal Data Protection Law in confronting data coloniality in Brazil, especially in light of the activities of large transnational digital platforms and Brazil's dependence on foreign technological infrastructures. It starts from the hypothesis that, although the LGPD represents a relevant normative advance in the protection of data subjects, it is not sufficient, by itself, to contain extractive practices based on the massive collection, processing, and monetization of personal data. To develop this analysis, the research adopts a qualitative approach, based on an interdisciplinary bibliographic review and a normative analysis of Brazilian legislation, in dialogue with authors who discuss imperialism, surveillance capitalism, data colonialism, coloniality of power, epistemicide, and digital sovereignty. The study first examines the economic and material concentration of digital infrastructures, showing that the so-called "cloud" depends on submarine cables, data centers, servers, energy, natural resources, and private property regimes. It then analyzes the limits of the LGPD regarding consent, informational self-determination, the role of the Brazilian Data Protection Authority, cross-border data flows, and the dependence on foreign platforms in strategic sectors such as education, health, the judiciary, and public administration. Finally, it discusses alternatives for building democratic digital sovereignty in Brazil, based on a dialogue with international regulatory references, especially the GDPR and the PIPL, the hacker-Fanonian critique, and proposals aimed at strengthening public infrastructure, algorithmic transparency, strategic public procurement, and critical digital education. The research concludes that the LGPD is necessary but insufficient to confront data coloniality, making it essential to connect it to a broader project of technological autonomy, social control, and digital sovereignty.

Keywords: data colonialism; digital sovereignty; LGPD; Big Techs; personal data protection.

SUMÁRIO

1 INTRODUÇÃO	7
2 CAPÍTULO I - COLONIALISMO DE DADOS E IMPERIALISMO DIGITAL	10
2.1 Do imperialismo clássico aos monopólios digitais contemporâneos	11
2.2 A Materialidade do Império das Nuvens: Hardware, cabos submarinos e a infraestrutura física da extração.....	12
2.3 Capitalismo de Vigilância: A experiência humana como matéria-prima para o lucro	14
2.4 Colonialismo de Dados: a apropriação da vida pelas relações digitais	16
2.5 Colonialidade do Poder e Epistemicídio: A lógica do Norte Global sobre o Sul Global	18
3 CAPÍTULO II - A LGPD FRENTE ÀS PRÁTICAS EXTRATIVISTAS	21
3.1 Acumulação Primitiva de Dados: A conversão da vida em ativos econômicos.....	21
3.2 Análise Crítica da LGPD: O consentimento como ilusão e os limites da autodeterminação informacional	23
3.3 A ANPD e o desafio de regular plataformas digitais globais.....	25
3.4 Impactos na Soberania Nacional: Fluxo transfronteiriço e a dependência de servidores estrangeiros.....	28
3.5 Manifestações da colonialidade de dados no contexto brasileiro.....	30
4 CAPÍTULO III - ESTRATÉGIAS DE DESCOLONIZAÇÃO E SOBERANIA DIGITAL	34
4.1 Referências regulatórias internacionais: PIPL chinesa e GDPR europeu como contrapontos à LGPD	35
4.2 Crítica Hacker-Fanoniana: Descolonizando a tecnologia e a soberania algorítmica ..	38
4.3 Propostas para a soberania digital brasileira: Nuvem pública nacional, armazenamento local de dados sensíveis e educação digital.....	41
5 CONCLUSÃO.....	45
REFERÊNCIAS	48

1 INTRODUÇÃO

A transformação digital das últimas décadas alterou profundamente as formas de produção, circulação e acumulação de riqueza na sociedade contemporânea. Nesse contexto, os dados pessoais passaram a ocupar posição estratégica na economia global, tornando-se recursos centrais para o desenvolvimento de tecnologias, algoritmos, sistemas de inteligência artificial e modelos de negócio baseados na coleta, análise e comercialização de informações em larga escala. Conforme observa Zuboff, consolidou-se um modelo econômico fundamentado na extração sistemática da experiência humana, convertida em dados comportamentais destinados à previsão e à modificação de condutas individuais (ZUBOFF, 2021, p. 25-26).

Essa nova dinâmica econômica não pode ser compreendida apenas como um avanço tecnológico. Diversos autores têm argumentado que as atuais formas de apropriação de dados reproduzem lógicas históricas de dominação características do colonialismo. Para Couldry e Mejías, o colonialismo de dados representa uma nova etapa da expansão capitalista, na qual a vida social passa a ser continuamente capturada e transformada em matéria-prima para processos de acumulação econômica (COULDRY; MEJIAS, 2019a, p. 337-339). Assim como o colonialismo clássico apropriava territórios, recursos naturais e força de trabalho, o colonialismo contemporâneo apropria-se de informações, comportamentos, relações sociais e experiências humanas.

A compreensão desse fenômeno encontra fundamento nas reflexões de Aníbal Quijano acerca da colonialidade do poder. Segundo o autor, o fim das administrações coloniais não significou o desaparecimento das estruturas de dominação construídas durante a modernidade, mas sua reorganização em novas formas de controle econômico, político, cultural e epistemológico (QUIJANO, 2009, p. 73-76). Nesse sentido, as relações de dependência observadas no ambiente digital podem ser interpretadas como expressões contemporâneas da colonialidade, uma vez que mantêm países periféricos em posição subordinada.

No contexto brasileiro, Silveira, Cassino e Souza sustentam que a captura massiva de dados por grandes plataformas digitais reproduz mecanismos de dependência tecnológica e econômica (SILVEIRA; CASSINO; SOUZA, 2021, p. 41-48). Assim, a extração contínua de informações pessoais, associada ao controle privado de infraestruturas digitais e algoritmos, favorece a concentração de poder em corporações transnacionais. Como resultado, países como o Brasil tornam-se fornecedores de matéria-prima informacional, enquanto o valor

econômico gerado a partir desses dados é apropriado predominantemente por empresas sediadas nos países do Norte Global.

Além disso, a concentração desse poder digital também pode ser analisada à luz da teoria do imperialismo desenvolvida por Lênin. Para o autor, a fase monopolista do capitalismo caracteriza-se pela crescente concentração da produção e do capital em grandes conglomerados econômicos capazes de controlar setores estratégicos da economia (LÊNIN, 2021, p. 114-120). Embora formulada em contexto histórico distinto, essa interpretação oferece instrumentos relevantes para compreender a atual centralização da infraestrutura digital, do processamento de dados, da inteligência artificial e dos serviços em nuvem em um número reduzido de empresas.

Paralelamente, Fanon demonstra que os sistemas de dominação não se limitam à exploração econômica, mas também operam por meio da imposição de estruturas de poder que condicionam a autonomia dos povos colonizados (FANON, 2022, p. 31-33). No ambiente digital, essa lógica manifesta-se na dependência técnica e epistemológica, na assimetria de acesso ao conhecimento e na dificuldade de controle sobre fluxos informacionais que atravessam fronteiras nacionais sem efetiva supervisão dos Estados do Sul Global.

Diante desse cenário, torna-se relevante investigar a capacidade do ordenamento jurídico brasileiro de enfrentar essas novas formas de dominação digital. A Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709/2018, representa o principal instrumento normativo voltado à proteção dos dados pessoais no país, estabelecendo princípios, direitos e mecanismos de responsabilização para agentes de tratamento (BRASIL, 2018, arts. 1º, 2º e 6º). Contudo, questiona-se se a legislação é suficiente para enfrentar estruturas globais de poder que operam para além da simples proteção individual da privacidade.

Nesse contexto, o debate não se restringe ao Brasil, pois a proteção de dados pessoais tornou-se uma questão central na agenda regulatória internacional, assumindo funções distintas conforme o modelo de governança digital adotado por cada Estado. O Regulamento Geral de Proteção de Dados da União Europeia, por exemplo, consolidou uma matriz normativa orientada pela proteção dos direitos fundamentais, pela limitação do tratamento de dados e pela responsabilização dos agentes públicos e privados (UNIÃO EUROPEIA, 2016, arts. 3º, 44-46 e 83). A experiência chinesa, especialmente a partir da Personal Information Protection Law, por sua vez, articula a proteção de informações pessoais a mecanismos mais amplos de controle de fluxos transfronteiriços, armazenamento territorial de dados e fortalecimento da capacidade regulatória estatal (CHINA, 2021, arts. 36, 38-40 e 66). Esse diálogo, que será aprofundado no desenvolvimento do trabalho, evidencia que a proteção de

dados pode ser concebida não apenas como tutela individual da privacidade, mas também como instrumento de soberania tecnológica e organização estratégica da economia digital.

Diante disso, a presente pesquisa parte do seguinte problema: em que medida a Lei Geral de Proteção de Dados é capaz de enfrentar a colonialidade de dados no Brasil, considerando que a extração, monetização e circulação de dados pessoais por grandes plataformas digitais ocorre em um contexto de baixa transparência efetiva, reduzido benefício local e limitada autonomia dos titulares diante de estruturas globais de concentração econômica, dependência tecnológica e controle informacional?

A hipótese adotada é que a LGPD, embora represente importante avanço na proteção de dados pessoais, não estabelece mecanismos suficientemente robustos para confrontar o poder econômico, tecnológico e informacional das grandes plataformas digitais. Inserida em um contexto de racionalidade neoliberal, concentração econômica e forte assimetria entre agentes reguladores nacionais e corporações transnacionais, a legislação tende a compatibilizar a proteção formal dos titulares com a continuidade dos modelos de negócio baseados na extração e monetização massiva de dados. Dessa forma, a LGPD acaba permitindo a permanência de práticas que reforçam relações de dependência tecnológica e limitam a soberania digital brasileira, transformando informações pessoais em commodities digitais sem que os titulares exerçam controle efetivo sobre seu uso, circulação e apropriação econômica (SILVEIRA; CASSINO; SOUZA, 2021, p. 55).

Dessa maneira, o objetivo geral desta pesquisa consiste em compreender como a LGPD, apesar de seu propósito protetivo, apresenta limitações no enfrentamento da colonialidade de dados no Brasil, permitindo a continuidade de práticas extrativistas promovidas por grandes empresas de tecnologia. Para tanto, serão analisados os conceitos de colonialismo de dados, colonialidade do poder, capitalismo de vigilância e soberania digital, buscando identificar os limites da legislação brasileira e discutir possíveis caminhos para o fortalecimento da autonomia tecnológica e informacional nacional.

2 CAPÍTULO I - COLONIALISMO DE DADOS E IMPERIALISMO DIGITAL

Antes de examinar os limites da Lei Geral de Proteção de Dados, é necessário compreender a estrutura econômica, tecnológica e epistemológica na qual a circulação contemporânea de dados está inserida. A colonialidade de dados não se manifesta apenas na coleta de informações pessoais, mas em um conjunto mais amplo de relações de poder que envolve concentração econômica, controle de infraestruturas digitais, extração de valor comportamental e produção assimétrica de conhecimento. Por isso, a análise da LGPD exige uma fundamentação teórica capaz de ultrapassar a dimensão estritamente normativa da proteção de dados.

O presente capítulo tem por objetivo construir essa base conceitual. Inicialmente, parte-se da teoria do imperialismo de Lênin, a fim de compreender como a concentração monopolista do capital permite interpretar a centralização contemporânea do poder tecnológico em grandes corporações transnacionais (LÊNIN, 2021, p. 116-120). Em seguida, discute-se a materialidade da chamada “nuvem”, evidenciando que a economia digital depende de cabos submarinos, data centers, servidores, energia, recursos naturais e trabalho humano, conforme apontam Faustino e Lippold ao analisarem o “Império das Nuvens” (FAUSTINO; LIPPOLD, 2023, p. 119-120).

Na sequência, são examinadas as contribuições de Shoshana Zuboff acerca do capitalismo de vigilância, especialmente no que se refere à transformação da experiência humana em dados comportamentais e produtos de predição (ZUBOFF, 2021, p. 25-26). Esse debate é aprofundado a partir da teoria do colonialismo de dados de Nick Couldry e Ulises Mejías, segundo a qual as relações sociais passam a ser continuamente capturadas e convertidas em matéria-prima para novos processos de acumulação econômica (COULDRY; MEJIAS, 2019a, p. 337-339).

Por fim, o capítulo articula essa discussão às reflexões de Aníbal Quijano, Frantz Fanon, Paola Ricaurte e Ramón Grosfoguel, a fim de demonstrar que a colonialidade digital envolve também a produção de hierarquias epistemológicas. Assim, a concentração dos meios de coleta, processamento e interpretação de dados não constitui apenas um problema econômico ou técnico, mas também uma forma de controle sobre os modos legítimos de produzir conhecimento, classificar populações e organizar a vida social (RICAURTE, 2019, p. 352-354). Essa fundamentação permitirá compreender, nos capítulos seguintes, por que a proteção jurídica dos dados pessoais, embora indispensável, mostra-se insuficiente quando dissociada de uma política mais ampla de soberania digital.

2.1 Do imperialismo clássico aos monopólios digitais contemporâneos

A compreensão do poder exercido pelas Big Techs exige situá-las dentro da evolução histórica do capitalismo e de suas formas de concentração econômica. Nesse sentido, a teoria do imperialismo desenvolvida por Lênin oferece instrumentos relevantes para analisar a centralização contemporânea do poder tecnológico. Para o autor, o imperialismo corresponde a uma etapa específica do capitalismo, marcada pela substituição progressiva da livre concorrência pelo domínio dos monopólios, pela fusão entre capital bancário e industrial e pela formação do capital financeiro, que passa a exercer influência decisiva sobre setores estratégicos da economia (LÊNIN, 2021, p. 69-80).

Segundo Lênin, a concentração da produção e do capital atinge níveis tão elevados que permite o surgimento de empresas capazes de controlar ramos inteiros da atividade econômica. Nessa dinâmica, as desigualdades entre empresas, setores produtivos e países não constituem desvios ocasionais do sistema, mas expressões do próprio desenvolvimento desigual do capitalismo em sua fase monopolista. A expansão capitalista, portanto, não elimina assimetrias, mas tende a reorganizá-las em novas formas de dependência entre centros econômicos dominantes e regiões periféricas (LÊNIN, 2021, p. 116-120).

A partir dessa lógica, a disputa entre potências deixa de ocorrer apenas pela conquista de territórios ainda não incorporados ao sistema capitalista mundial e passa a envolver o controle monopolista de espaços, mercados e recursos já integrados à economia global. Como observa Lênin:

A partilha do mundo é a transição de uma política colonial que se estendeu sem obstáculos às regiões ainda não apropriadas por nenhuma potência capitalista para uma política colonial de posse monopolista dos territórios da Terra, já inteiramente repartida. (LÊNIN, 2021, p. 114).

Embora formulada no início do século XX, essa interpretação permanece relevante para compreender novas formas de concentração econômica produzidas pela economia digital. Atualmente, corporações como Alphabet, Meta, Amazon, Apple e Microsoft ocupam posição central na organização do ambiente informacional, pois controlam plataformas digitais, sistemas operacionais, serviços de computação em nuvem, infraestrutura de armazenamento, modelos de inteligência artificial e mecanismos de mediação da vida social. Essa centralidade permite que tais empresas não apenas ofereçam serviços tecnológicos, mas também organizem os meios pelos quais dados são coletados, processados, circulam e são monetizados.¹

¹ MURPHY; TUCKER, 2025.

A partir dessa perspectiva, é possível compreender as Big Techs como expressões contemporâneas da lógica monopolista analisada por Lênin, ainda que em condições históricas distintas. Se, no imperialismo clássico, a concentração econômica estava associada ao controle de territórios, recursos naturais, mercados e rotas comerciais, no capitalismo digital ela passa a envolver também o domínio sobre infraestruturas informacionais, fluxos de dados, capacidade computacional e sistemas algorítmicos. A disputa por poder econômico, portanto, desloca-se parcialmente para o controle dos meios técnicos que estruturam a circulação da informação e a produção de conhecimento na sociedade contemporânea.

Nesse contexto, os dados assumem função estratégica. Eles não substituem integralmente recursos clássicos como petróleo, minerais ou força de trabalho, mas passam a integrar os processos contemporâneos de acumulação como ativos capazes de alimentar modelos preditivos, sistemas de inteligência artificial, publicidade direcionada e mecanismos de influência comportamental. Dessa forma, a lógica monopolista não desaparece com a digitalização da economia, ao contrário, atualiza-se em torno do controle privado das infraestruturas e dos fluxos informacionais que sustentam a vida social contemporânea.

Assim, o imperialismo contemporâneo assume características distintas daquelas observadas no período colonial clássico, sem abandonar sua lógica fundamental de concentração, hierarquização e dependência. A centralização do poder nas Big Techs, a dependência tecnológica dos países periféricos e a apropriação privada dos dados produzidos globalmente constituem elementos fundamentais para compreender o surgimento do colonialismo de dados. A teoria leninista do imperialismo não é utilizada aqui como explicação suficiente da economia digital, mas como ponto de partida para compreender como a lógica monopolista do capitalismo se atualiza diante das tecnologias informacionais do século XXI.

2.2 A Materialidade do Império das Nuvens: Hardware, cabos submarinos e a infraestrutura física da extração

A metáfora da “nuvem” frequentemente sugere um espaço abstrato, leve e descentralizado, no qual dados circulam livremente em um ambiente virtual aparentemente desvinculado de limitações físicas. Contudo, essa representação oculta as bases materiais que sustentam a economia digital contemporânea. O armazenamento, o processamento e a transmissão de informações dependem de uma extensa infraestrutura composta por cabos submarinos de fibra óptica, servidores, sistemas de refrigeração, redes elétricas e grandes centros de processamento de dados distribuídos pelo planeta. Longe de constituir uma

dimensão puramente imaterial, a chamada nuvem aproxima-se de um complexo industrial global, dependente de elevados investimentos, recursos naturais, energia e trabalho humano.

Nesse sentido, Deivison Faustino e Walter Lippold chamam atenção para aquilo que denominam “Império das Nuvens”, expressão utilizada para evidenciar a dimensão material frequentemente invisibilizada das tecnologias digitais. Não há software sem hardware, nem inteligência artificial sem infraestrutura física. A aparente instantaneidade das interações digitais somente é possível porque existe uma rede concreta de equipamentos, cabos, servidores, data centers e sistemas energéticos capazes de manter em funcionamento permanente as plataformas que organizam parcela crescente da vida social. (FAUSTINO; LIPPOLD, 2023, p. 119-120).

A relevância dessa materialidade pode ser observada no projeto de instalação de um data center vinculado ao TikTok no município de Caucaia, no estado do Ceará. Segundo reportagem do Intercept Brasil, baseada em documento interno obtido pelo veículo, o empreendimento poderia consumir, em sua fase inicial, energia equivalente ao consumo residencial diário de aproximadamente 2,2 milhões de brasileiros, além de demandar cerca de 30 mil litros de água por dia para seu funcionamento (MARTINS; AMORIM, 2025). O caso evidencia que a circulação global de dados depende de estruturas fisicamente situadas, capazes de produzir impactos ambientais, territoriais e sociais em comunidades específicas.

Esse exemplo é particularmente relevante porque demonstra que a economia digital também se apoia em desigualdades territoriais. A instalação de grandes centros de processamento em regiões periféricas pode ser apresentada como modernização tecnológica ou atração de investimentos, mas envolve disputas concretas por energia, água, solo, incentivos públicos e licenciamento ambiental. Assim, a infraestrutura que sustenta plataformas globais não se limita a beneficiar os territórios onde é instalada, ela também pode aprofundar conflitos locais, especialmente quando comunidades afetadas possuem baixa participação nas decisões sobre os empreendimentos destinados a atender demandas informacionais de corporações transnacionais.

Além dos data centers, a infraestrutura digital contemporânea depende de extensas redes de cabos submarinos responsáveis por conectar continentes e possibilitar o fluxo internacional de dados. Embora a internet seja frequentemente associada à ideia de descentralização, sua operação depende de corredores físicos altamente estratégicos, cuja construção e controle envolvem vultosos investimentos privados. Nos últimos anos, empresas como Google, Meta, Amazon e Microsoft passaram a desempenhar papel crescente nesse setor, participando diretamente da construção e financiamento de rotas internacionais de

transmissão de dados. Essa transformação amplia a capacidade das grandes plataformas de controlar não apenas serviços digitais, mas também parte da infraestrutura que viabiliza sua circulação global.²

Nesse contexto, a questão central deixa de ser apenas a existência dessa infraestrutura e passa a envolver sua propriedade, localização e controle. Em uma sociedade cada vez mais dependente do processamento de dados, os atores capazes de financiar, construir e operar cabos, servidores e data centers ocupam posições privilegiadas na organização dos fluxos informacionais globais. Desse modo, a materialidade da nuvem revela que o ambiente digital não está dissociado das relações de poder que atravessam a economia contemporânea, mas constitui uma de suas expressões mais estratégicas.

A compreensão dessa infraestrutura física é fundamental para a análise da colonialidade de dados. Se os dados são extraídos de forma massiva da vida cotidiana, sua circulação e monetização dependem de redes materiais controladas por agentes econômicos específicos. Portanto, discutir soberania digital exige observar não apenas normas jurídicas de proteção de dados, mas também quem controla os meios técnicos responsáveis por armazenar, processar e transportar as informações que sustentam a economia digital.

2.3 Capitalismo de Vigilância: A experiência humana como matéria-prima para o lucro

A compreensão da economia digital contemporânea exige examinar os mecanismos por meio dos quais a experiência humana é convertida em valor econômico. Nesse sentido, Shoshana Zuboff desenvolve o conceito de capitalismo de vigilância para descrever uma nova lógica de acumulação baseada na apropriação sistemática de dados comportamentais. Segundo a autora, esse modelo reivindica unilateralmente a experiência humana como matéria-prima gratuita, transformando atividades cotidianas em informações passíveis de extração, processamento e monetização (ZUBOFF, 2021, p. 25-26).

Inicialmente, parte dos dados coletados pelas plataformas digitais é utilizada para o aprimoramento de produtos e serviços. Contudo, uma parcela significativa dessas informações excede as necessidades operacionais imediatas das plataformas, constituindo aquilo que Zuboff denomina superávit comportamental. Esse excedente não é descartado, mas processado por sistemas de inteligência de máquina e convertido em produtos de predição, voltados a antecipar comportamentos presentes e futuros dos indivíduos (ZUBOFF, 2021, p. 151).

² BADSHAH, 2025; WEATHERBED, 2024.

A partir dessa dinâmica, as previsões sobre condutas humanas passam a ser comercializadas nos chamados mercados de comportamentos futuros. O valor econômico das plataformas não decorre apenas da coleta de dados, mas da capacidade de transformar hábitos, preferências, emoções, deslocamentos e interações sociais em probabilidades calculáveis e negociáveis. Assim, a experiência humana passa a integrar diretamente os processos de acumulação de capital, não apenas como informação armazenada, mas como base para a produção de previsões economicamente úteis (ZUBOFF, 2021, p. 147-150).

Entretanto, a lógica do capitalismo de vigilância não se limita à observação passiva dos indivíduos. À medida que a competição por previsões mais precisas se intensifica, torna-se economicamente vantajoso não apenas conhecer comportamentos, mas também influenciá-los. Nesse contexto, as plataformas passam a desenvolver mecanismos de indução, direcionamento e modulação de condutas, organizando ambientes digitais capazes de estimular determinadas ações e reduzir a incerteza sobre o comportamento dos usuários. Dessa forma, a coleta de dados articula-se progressivamente à intervenção sobre a própria experiência social.

É nesse cenário que Zuboff identifica a emergência do poder instrumentário. Diferentemente de formas tradicionais de dominação política, esse poder opera por meio de arquiteturas computacionais distribuídas em plataformas, aplicativos, sensores, dispositivos conectados e sistemas algorítmicos. Seu objetivo não é apenas vigiar indivíduos em sentido clássico, mas conhecer, prever e orientar comportamentos em escala, produzindo novas formas de assimetria entre aqueles que fornecem dados continuamente e aqueles que controlam os meios de sua análise e utilização (ZUBOFF, 2021, p. 25).

Essa dinâmica produz profundas desigualdades de conhecimento e poder. As plataformas acumulam vastos domínios de informação derivados da experiência humana, enquanto os usuários permanecem, em grande medida, alheios aos processos de coleta, cruzamento, interpretação e utilização econômica de seus próprios dados. O conhecimento produzido a partir das interações sociais não retorna aos indivíduos de maneira proporcional, mas é apropriado por agentes privados capazes de convertê-lo em vantagem econômica, capacidade preditiva e influência comportamental.

Dessa forma, o capitalismo de vigilância não se limita à publicidade direcionada ou à coleta massiva de informações pessoais. Trata-se de uma lógica econômica que transforma a experiência humana em recurso estratégico, ampliando a capacidade das plataformas digitais de conhecer, prever e influenciar a vida social. A centralidade assumida pelos dados nesse

processo constitui elemento fundamental para compreender, no tópico seguinte, a formulação do colonialismo de dados como uma nova etapa de apropriação da vida pelas relações digitais.

2.4 Colonialismo de Dados: a apropriação da vida pelas relações digitais

As reflexões desenvolvidas por Shoshana Zuboff acerca do capitalismo de vigilância encontram aprofundamento na teoria do colonialismo de dados formulada por Nick Couldry e Ulises Mejías. Enquanto Zuboff evidencia a lógica econômica por meio da qual a experiência humana é convertida em dados comportamentais, produtos de predição e capacidade de influência, Couldry e Mejías ampliam essa análise ao situar a apropriação de dados em uma história mais longa de expansão capitalista e dominação colonial. Para os autores, o colonialismo de dados não constitui mera metáfora, mas uma nova ordem social baseada na apropriação sistemática da vida humana para fins de acumulação econômica (COULDRY; MEJIAS, 2019a, p. 337-339).

Assim como o colonialismo histórico transformou territórios, recursos naturais e populações em objetos de exploração, o colonialismo de dados inaugura mecanismos voltados à captura contínua da experiência humana por meio das tecnologias digitais. A diferença fundamental está no objeto prioritário da apropriação: se o colonialismo clássico se organizava em torno da ocupação territorial, da extração de recursos e da exploração direta do trabalho, o colonialismo contemporâneo passa a incidir sobre relações sociais, comportamentos, comunicações, deslocamentos, preferências e interações cotidianas. Desse modo, a vida social passa a ser tratada como fonte permanente de dados economicamente exploráveis (COULDRY; MEJIAS, 2019a, p. 337-339).

Esse processo ocorre por meio daquilo que Couldry e Mejías denominam *data relations*, ou relações de dados. Trata-se de formas de organização social que tornam a produção contínua de dados uma condição ordinária da vida contemporânea. Interações em redes sociais, buscas online, compras, deslocamentos, uso de aplicativos, atividades profissionais e formas de comunicação passam a ser permanentemente registradas, processadas e integradas a sistemas de análise. As relações de dados não se limitam a ferramentas tecnológicas específicas, mas constituem uma nova forma de mediação da vida social, na qual participar de ambientes digitais implica produzir informações passíveis de captura, classificação e monetização.

A força do colonialismo de dados reside justamente em sua aparência de normalidade. A extração de informações ocorre de forma incorporada a práticas cotidianas, muitas vezes apresentadas como conveniência, personalização, eficiência ou acesso gratuito a serviços

digitais. Entretanto, por trás dessa aparente naturalidade, consolida-se uma estrutura assimétrica em que os usuários produzem continuamente dados, enquanto as plataformas concentram os meios técnicos, econômicos e cognitivos necessários para interpretá-los e convertê-los em valor. Assim, a exploração não depende apenas de coerção direta, mas da incorporação da vida social a ambientes digitais desenhados para capturar e processar informações em escala.

A originalidade da formulação de Couldry e Mejías está na identificação de uma continuidade histórica entre as lógicas coloniais do passado e as formas contemporâneas de exploração digital. Embora os objetos da apropriação tenham se transformado, permanece a dinâmica pela qual dimensões da vida antes não plenamente integradas aos circuitos econômicos passam a ser incorporadas aos processos de acumulação. Nesse sentido, o colonialismo de dados representa uma expansão das fronteiras do capital sobre a experiência humana, convertendo relações sociais em recursos informacionais e reforçando assimetrias entre aqueles que produzem dados e aqueles que controlam sua interpretação, circulação e uso econômico (COULDRY; MEJIAS, 2019a, p. 337-339).

No contexto brasileiro, essa leitura dialoga com as reflexões de Silveira, Cassino e Souza, para quem a captura massiva de dados por grandes plataformas digitais aprofunda relações de dependência tecnológica e econômica em países periféricos (SILVEIRA; CASSINO; SOUZA, 2021, p. 41-48). A apropriação dos dados produzidos socialmente não ocorre em condições de igualdade, pois depende de infraestruturas, plataformas, algoritmos e capacidades analíticas concentradas em corporações transnacionais. Dessa forma, países como o Brasil participam da economia digital em posição subordinada, fornecendo fluxos contínuos de informações que são processados e monetizados por agentes externos.

Dessa forma, o colonialismo de dados não representa apenas uma nova dinâmica de acumulação econômica, mas também uma reconfiguração das relações de poder na sociedade contemporânea. A concentração dos meios de coleta, processamento e interpretação de dados produz assimetrias profundas entre aqueles que vivem, comunicam-se e interagem em ambientes digitais e aqueles que controlam os sistemas responsáveis por transformar essas experiências em conhecimento operacional e valor econômico. Essa dimensão permite aproximar a discussão das reflexões sobre colonialidade do poder, dependência e epistemicídio, desenvolvidas no tópico seguinte a partir de Aníbal Quijano, Frantz Fanon, Paola Ricaurte e Ramón Grosfoguel.

2.5 Colonialidade do Poder e Epistemicídio: A lógica do Norte Global sobre o Sul Global

As transformações analisadas nos tópicos anteriores não podem ser compreendidas apenas como fenômenos econômicos ou tecnológicos. A concentração da infraestrutura digital, da capacidade de processamento de dados e da produção de conhecimento sobre populações inteiras insere-se em estruturas históricas mais amplas de poder. Nesse sentido, a teoria da colonialidade do poder, desenvolvida por Aníbal Quijano, oferece instrumentos fundamentais para compreender a permanência de relações de dominação que sobrevivem ao fim do colonialismo formal (QUIJANO, 2009, p. 73-76).

Segundo Quijano, a modernidade não pode ser dissociada da colonização, pois o sistema-mundo moderno foi construído a partir da imposição de hierarquias econômicas, políticas, culturais e epistemológicas que posicionaram a Europa como centro legítimo da produção de conhecimento e do exercício do poder. Mesmo após os processos de independência política das antigas colônias, tais estruturas continuaram operando por meio da colonialidade do poder, compreendida como um padrão duradouro de dominação que organiza as relações globais entre centros e periferias (QUIJANO, 2009, p. 73-76).

Essa dimensão epistemológica da colonialidade é aprofundada por Ramón Grosfoguel ao discutir a formação das estruturas modernas de conhecimento. Para o autor, a modernidade ocidental não se consolidou apenas por meio da conquista territorial, da exploração econômica e da dominação política, mas também pela destruição e inferiorização de conhecimentos produzidos por povos colonizados, mulheres e sujeitos situados fora do padrão europeu de racionalidade. Nesse sentido, os genocídios coloniais foram acompanhados por epistemicídios, isto é, pela desqualificação sistemática de formas de saber, espiritualidade, memória e organização social que não se adequavam ao modelo moderno-colonial de conhecimento (GROSFOGUEL, 2016, p. 25-27).

A partir dessa leitura, o epistemicídio não deve ser compreendido apenas como apagamento abstrato de ideias, mas como parte de uma estrutura histórica que define quais sujeitos podem produzir conhecimento válido e quais permanecem reduzidos à condição de objetos de observação, classificação e intervenção. Essa hierarquia epistêmica permite compreender por que a racionalidade moderna frequentemente se apresenta como universal, embora esteja enraizada em experiências históricas particulares do Norte Global. No contexto digital, essa lógica reaparece quando plataformas, algoritmos e sistemas de dados passam a classificar populações, organizar visibilidades e definir padrões de normalidade a partir de modelos técnicos e epistemológicos produzidos por centros hegemônicos de poder.

Essa leitura é especialmente relevante para compreender a colonialidade de dados. Conforme observa Paola Ricaurte, a ordem social, política e econômica do colonialismo de dados emerge da própria matriz colonial, reproduzindo relações históricas de dominação por meio do extrativismo digital (RICAURTE, 2019, p. 352-354). Nesse modelo, a vida humana é continuamente convertida em fluxos de dados destinados à extração de valor, ampliando processos de marginalização e desigualdade, especialmente em sociedades marcadas por experiências coloniais e profundas assimetrias sociais.

Para Ricaurte, esse cenário é sustentado por uma epistemologia centrada em dados, baseada na premissa de que os dados representam a forma mais objetiva, eficiente e valiosa de produzir conhecimento sobre a realidade. Como consequência, formas alternativas de compreender, narrar e organizar o mundo tendem a ser deslegitimadas ou subordinadas a modelos produzidos por grandes centros tecnológicos. Assim, a racionalidade orientada por dados não apenas registra a realidade, mas também participa da definição dos critérios pelos quais sujeitos, comportamentos e territórios passam a ser classificados, mensurados e governados (RICAURTE, 2019, p. 352-354).

Nesse contexto, as reflexões de Frantz Fanon contribuem para aprofundar a análise ao demonstrar que os processos coloniais não se limitam à exploração econômica dos territórios dominados, mas produzem formas duradouras de dependência material, cultural e subjetiva (FANON, 2022, p. 31-33). A promessa de universalidade frequentemente oculta relações assimétricas nas quais determinados grupos são reconhecidos como produtores legítimos de conhecimento, enquanto outros têm sua autonomia negada ou condicionada por estruturas externas de poder. Sob essa perspectiva, a expansão das tecnologias digitais pode reproduzir mecanismos semelhantes, na medida em que concentra capacidades técnicas e cognitivas em determinados centros e restringe a autonomia tecnológica das regiões periféricas.

A própria infraestrutura que sustenta a economia digital evidencia essas contradições. Como discutido anteriormente, a extração de minerais estratégicos, o consumo energético de data centers, a dependência de cabos submarinos, servidores e sistemas de computação em nuvem demonstram que a inovação tecnológica não se realiza em um espaço abstrato, mas depende de cadeias materiais distribuídas de maneira desigual. Como observam Faustino e Lippold, a materialidade do chamado “Império das Nuvens” apoia-se em estruturas globais que conectam tecnologia, recursos naturais, trabalho humano e relações históricas de exploração (FAUSTINO; LIPPOLD, 2023, p. 119-120).

Dessa forma, o colonialismo de dados manifesta-se não apenas na extração massiva de informações pessoais, mas também na concentração dos meios de produção do conhecimento,

na definição dos padrões tecnológicos considerados legítimos e na reprodução de estruturas históricas de dependência entre centros e periferias. Essa colonialidade manifesta-se na capacidade de determinados atores coletarem, interpretarem e utilizarem dados em escala global, enquanto outros permanecem limitados à condição de fornecedores de recursos, informações e experiências. Compreender essa dimensão é fundamental para analisar, no capítulo seguinte, os limites da Lei Geral de Proteção de Dados diante das assimetrias estruturais que caracterizam a economia digital contemporânea.

3 CAPÍTULO II - A LGPD FRENTE ÀS PRÁTICAS EXTRATIVISTAS

Após a construção do referencial teórico sobre imperialismo digital, capitalismo de vigilância, colonialismo de dados e colonialidade do poder, torna-se necessário examinar em que medida a Lei Geral de Proteção de Dados é capaz de enfrentar essas dinâmicas no contexto brasileiro. A LGPD constitui o principal marco normativo nacional voltado à proteção de dados pessoais, estabelecendo princípios, direitos dos titulares, bases legais, deveres aos agentes de tratamento, mecanismos de fiscalização e hipóteses de responsabilização. Contudo, sua eficácia deve ser analisada à luz das assimetrias econômicas, técnicas e informacionais que estruturam a economia digital contemporânea.

Nesse sentido, este capítulo analisa os limites da LGPD diante de práticas extrativistas baseadas na coleta, no processamento, na circulação e na monetização massiva de dados pessoais. Inicialmente, examina-se a noção de acumulação primitiva de dados, a fim de demonstrar como a vida cotidiana é convertida em ativo econômico. Em seguida, discute-se criticamente o consentimento e a autodeterminação informacional, destacando as dificuldades de controle efetivo pelos titulares em ambientes digitais marcados por opacidade e dependência. Posteriormente, analisa-se o papel da ANPD, os desafios da fiscalização de plataformas globais, os fluxos transfronteiriços de dados e os impactos dessas dinâmicas sobre a soberania nacional. Por fim, são apresentadas manifestações concretas da colonialidade de dados no Brasil, especialmente em setores estratégicos como educação, saúde, Judiciário, administração pública e empresas públicas de tecnologia.

3.1 Acumulação Primitiva de Dados: A conversão da vida em ativos econômicos

A noção de acumulação primitiva de dados permite compreender como a economia digital transforma dimensões ordinárias da vida social em ativos informacionais economicamente exploráveis. Segundo Joyce Souza, o colonialismo de dados aponta para uma etapa de expansão capitalista marcada pela capitalização total da vida humana, na medida em que comportamentos, relações sociais, preferências, deslocamentos e experiências cotidianas passam a ser convertidos em ativos informacionais (SILVEIRA; CASSINO; SOUZA, 2021, p. 116). Assim como a acumulação primitiva clássica esteve associada à incorporação violenta de terras, corpos e recursos aos circuitos do capital, a economia digital contemporânea amplia suas fronteiras ao transformar dimensões ordinárias da existência em recursos economicamente exploráveis.

Essa dinâmica manifesta-se por meio da coleta contínua de dados realizada por redes sociais, mecanismos de busca, aplicativos, plataformas de comércio eletrônico, dispositivos conectados e sistemas de inteligência artificial. As informações produzidas pelos usuários deixam de possuir apenas valor funcional para a prestação de serviços e passam a alimentar modelos de publicidade direcionada, sistemas de recomendação, mecanismos de predição comportamental e estratégias de modulação de condutas. Nesse sentido, os dados tornam-se elementos centrais para a produção de valor na economia digital, pois possibilitam não apenas conhecer padrões sociais, mas também antecipar e influenciar comportamentos futuros (ZUBOFF, 2021, p. 146-148).

A acumulação primitiva de dados, portanto, não se realiza apenas pela coleta isolada de informações pessoais, mas pela incorporação contínua da própria vida social a sistemas técnicos de extração. Cada interação digital, deslocamento registrado, busca realizada, compra efetuada ou vínculo social mediado por plataformas pode ser convertido em informação economicamente útil. Essa lógica aproxima-se da formulação de Couldry e Mejías acerca das *data relations*, na medida em que a produção permanente de dados passa a constituir uma condição ordinária de participação na vida social contemporânea (COULDRY; MEJIAS, 2019b, p. 12-13).

Nesse cenário, a posição das grandes plataformas digitais torna-se particularmente estratégica. Quanto maior a capacidade de coletar, cruzar e interpretar informações sobre indivíduos e populações, maior também é sua vantagem econômica e política. A concentração de dados permite o aprimoramento de sistemas algorítmicos, o desenvolvimento de inteligência artificial, a ampliação de mercados preditivos e a consolidação de formas privadas de conhecimento sobre a sociedade. Assim, a acumulação de dados converte-se também em acumulação de poder informacional.

É justamente diante dessa realidade que se situa a Lei Geral de Proteção de Dados, como tentativa de estabelecer limites jurídicos para a utilização econômica das informações pessoais. Ao reconhecer direitos aos titulares e disciplinar as práticas de tratamento, a LGPD busca conter usos abusivos e assegurar maior controle sobre os dados pessoais (BRASIL, 2018, arts. 1º, 2º e 6º). Contudo, sua efetividade depende da capacidade de enfrentar modelos de negócio cuja lógica econômica está profundamente vinculada à coleta contínua, ao cruzamento massivo e à exploração comercial das informações produzidas pelos próprios titulares.

Dessa forma, antes de analisar especificamente os mecanismos previstos pela LGPD, torna-se necessário compreender como seus princípios dialogam com uma economia

estruturada pela extração massiva de dados. A partir dessa perspectiva, será possível avaliar em que medida a legislação brasileira é capaz de limitar práticas associadas à colonialidade de dados ou se acaba operando predominantemente como instrumento de regulação formal de uma dinâmica econômica já consolidada.

3.2 Análise Crítica da LGPD: O consentimento como ilusão e os limites da autodeterminação informacional

A Lei Geral de Proteção de Dados estrutura-se a partir de princípios e bases legais voltados à proteção dos titulares diante das atividades de tratamento de dados pessoais. Entre esses fundamentos, destaca-se a autodeterminação informativa, prevista no art. 2º da legislação, bem como a possibilidade de tratamento mediante consentimento do titular, nos termos dos arts. 5º, XII, 7º, I, e 8º da LGPD. Em tese, o consentimento deveria assegurar que o indivíduo pudesse decidir, de maneira livre, informada e inequívoca, sobre a utilização de suas informações pessoais, fortalecendo sua autonomia diante de agentes públicos e privados de tratamento (BRASIL, 2018, arts. 2º, 5º, XII, 7º, I, e 8º).

Entretanto, a efetividade desse modelo torna-se problemática quando observada à luz das estruturas econômicas e tecnológicas que caracterizam a economia digital contemporânea. O consentimento pressupõe a existência de condições minimamente equilibradas entre as partes, bem como a possibilidade real de compreensão das consequências decorrentes da coleta, do cruzamento e da utilização dos dados pessoais. Na prática, porém, os titulares frequentemente se deparam com contratos extensos, políticas de privacidade de difícil compreensão, linguagem técnica complexa e sistemas de tratamento cujas operações permanecem, em grande medida, inacessíveis ao público.

Nesse sentido, Shoshana Zuboff argumenta que os contratos de adesão das plataformas digitais funcionam como verdadeiros “termos de rendição”, por meio dos quais os usuários aceitam condições impostas unilateralmente para acessar serviços que se tornaram praticamente indispensáveis à vida social contemporânea (ZUBOFF, 2021, p. 347). A liberdade formal de escolha é limitada pelo papel central dessas plataformas na comunicação, no trabalho, no consumo, na educação e na participação social. Assim, a recusa ao consentimento pode significar a exclusão ou restrição de acesso a espaços essenciais da vida cotidiana, convertendo a autonomia do titular em uma escolha apenas aparente.

Essa crítica também encontra respaldo na doutrina brasileira especializada em proteção de dados. Bruno Bioni, ao analisar a função e os limites do consentimento, sustenta que a centralidade conferida a esse instituto revela uma contradição no próprio desenho

regulatório da proteção de dados pessoais. Embora a legislação reconheça uma situação específica de vulnerabilidade do titular, o modelo regulatório muitas vezes aposta na figura de um sujeito racional, livre e plenamente capaz de controlar o fluxo de suas informações em ambientes marcados por elevada complexidade técnica e forte assimetria informacional. Desse modo, o consentimento pode deixar de operar como instrumento efetivo de autodeterminação informacional e passar a atuar como mecanismo de legitimação dos modelos de negócio baseados na exploração econômica dos dados pessoais (BIONI, 2019, p. 180-181).

Essa dificuldade também se manifesta no campo da transparência. A LGPD estabelece, em seu art. 6º, princípios como finalidade, necessidade, adequação e transparência, exigindo que o tratamento de dados seja realizado de modo compatível com propósitos legítimos, específicos e informados ao titular (BRASIL, 2018, art. 6º). Contudo, o acesso formal a políticas de privacidade e termos de uso não significa, necessariamente, compreensão efetiva dos processos de tratamento. O titular pode ser informado sobre a existência da coleta, mas dificilmente possui condições de compreender como seus dados serão combinados, inferidos, compartilhados, utilizados para construção de perfis ou convertidos em valor econômico.

A opacidade algorítmica aprofunda esse problema. Ainda que a legislação assegure direitos relacionados ao acesso, correção, eliminação e informação sobre o tratamento de dados, os processos de análise, classificação e predição frequentemente permanecem protegidos por sigilo empresarial, complexidade técnica ou arquitetura fechada das plataformas. Dessa forma, o indivíduo pode conhecer parcialmente quais informações foram coletadas, mas raramente compreende os efeitos concretos de seu tratamento, especialmente quando seus dados são utilizados para alimentar sistemas de recomendação, publicidade direcionada, inteligência artificial ou mecanismos de influência comportamental.

Sob essa perspectiva, a crítica ao consentimento não significa negar sua importância jurídica, mas reconhecer seus limites diante da economia digital contemporânea. Como observa Bioni, a autodeterminação informativa não pode ser reduzida à simples manifestação individual de vontade, especialmente quando o titular dos dados se encontra em posição de hipervulnerabilidade diante de agentes econômicos capazes de estruturar unilateralmente os fluxos informacionais. Por isso, a proteção de dados exige não apenas mecanismos de escolha individual, mas também formas de intervenção jurídica capazes de limitar a própria circulação e exploração econômica das informações pessoais (BIONI, 2019, p. 175).

Dessa forma, embora a LGPD represente avanço relevante no reconhecimento dos direitos dos titulares, seus instrumentos revelam limitações diante de relações marcadas por profundas assimetrias de poder, informação e capacidade técnica. O consentimento, a transparência e a autodeterminação informativa permanecem indispensáveis, mas mostram-se insuficientes quando isolados de mecanismos capazes de enfrentar a opacidade algorítmica, a concentração econômica das plataformas e a dependência estrutural da sociedade em relação aos serviços digitais. Essa constatação permite compreender por que a proteção de dados, quando dissociada de uma política mais ampla de soberania digital, tende a regular formalmente práticas extrativistas sem alterar integralmente suas condições de possibilidade.

3.3 A ANPD e o desafio de regular plataformas digitais globais

A efetividade da Lei Geral de Proteção de Dados depende não apenas da existência de direitos formalmente assegurados aos titulares, mas também da capacidade institucional de fiscalizar seu cumprimento. Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) desempenha papel central na implementação da política brasileira de proteção de dados, sendo responsável por zelar pela proteção dos dados pessoais, editar normas e procedimentos, fiscalizar condutas, aplicar sanções administrativas e promover ações de orientação e educação, conforme previsto no art. 55-J da LGPD (BRASIL, 2018, art. 55-J).

A criação da ANPD representou avanço importante para a consolidação de um regime nacional de proteção de dados. Do mesmo modo, sua transformação em autarquia de natureza especial reforçou sua autonomia institucional e aproximou o modelo brasileiro de experiências regulatórias que exigem autoridades técnicas capazes de atuar com independência diante de agentes públicos e privados (BRASIL, 2022, art. 1º). Contudo, a existência formal de competências regulatórias não elimina, por si só, as assimetrias estruturais que atravessam a economia digital. Regular plataformas digitais globais exige capacidade técnica, estabilidade institucional, recursos humanos especializados, instrumentos de auditoria e poder sancionatório efetivamente dissuasório.

Essa dificuldade torna-se mais evidente quando se observa o perfil dos agentes regulados. Grandes plataformas digitais transnacionais concentram recursos econômicos, tecnológicos, jurídicos e informacionais em escala global, operando modelos de negócio baseados na coleta, no processamento e na monetização massiva de dados pessoais. Assim, a atuação de uma autoridade nacional passa a ser confrontada por empresas capazes de organizar fluxos informacionais complexos, distribuir operações entre diferentes jurisdições,

proteger algoritmos sob sigilo empresarial e mobilizar estruturas jurídicas sofisticadas para responder a investigações e processos administrativos.

A assimetria entre regulador e regulado não é apenas quantitativa, mas qualitativa. A ANPD não fiscaliza apenas violações pontuais de privacidade, mas sistemas técnicos que envolvem publicidade comportamental, inteligência artificial, decisões automatizadas, análise preditiva, compartilhamento massivo de dados e integração entre múltiplos serviços digitais. Nesse cenário, a fiscalização exige não apenas leitura jurídica da LGPD, mas também capacidade de compreender arquiteturas tecnológicas, cadeias de tratamento, modelos algorítmicos e práticas comerciais que frequentemente permanecem opacas ao titular e ao próprio Estado. Por essa razão, a atuação regulatória não pode limitar-se à verificação formal de políticas de privacidade, termos de uso ou bases legais declaradas pelos agentes de tratamento. É necessário avaliar como os sistemas efetivamente operam, quais fluxos informacionais são produzidos, quais inferências são realizadas e de que modo tais práticas afetam direitos, liberdades e a autonomia dos titulares.

A própria lógica sancionatória da LGPD revela limites diante desse cenário. O art. 52 da legislação prevê sanções administrativas como advertência, multa simples, multa diária, publicização da infração, bloqueio, eliminação de dados pessoais e outras medidas restritivas relacionadas ao tratamento de dados (BRASIL, 2018, art. 52). Embora tais instrumentos sejam juridicamente relevantes, sua eficácia depende da capacidade concreta de investigação, instrução processual, aplicação tempestiva e imposição de custos efetivos às empresas infratoras.

Diante de corporações cuja rentabilidade global se dá pela exploração intensiva de dados, sanções eventualmente tardias, isoladas ou economicamente absorvíveis podem perder parte de sua função dissuasória.³

Além disso, a atuação da ANPD tem combinado medidas de fiscalização, prevenção, orientação e promoção de cultura de proteção de dados. Essa estratégia pode ser compreendida como adequada em um ambiente regulatório ainda recente, especialmente diante da necessidade de orientar agentes públicos e privados sobre a aplicação da LGPD. Contudo, quando se trata de grandes plataformas digitais, mecanismos orientativos ou baseados na adequação voluntária podem mostrar-se insuficientes para enfrentar modelos de negócio profundamente dependentes da extração e monetização de dados pessoais.

³ MURPHY; TUCKER, 2025.

Essa tensão também é percebida na doutrina brasileira. Bruno Bioni observa que qualquer perspectiva regulatória em matéria de proteção de dados deve levar em consideração a existência de uma economia de vigilância, estruturada pela monetização e circulação contínua de dados pessoais (BIONI, 2019, p. 24). A partir dessa leitura, a fiscalização não pode se restringir à regularidade formal do tratamento, devendo considerar a lógica econômica que incentiva a coleta excessiva, o compartilhamento ampliado e a reutilização permanente das informações pessoais.

A situação torna-se ainda mais complexa quando se observa a crescente dependência de órgãos públicos em relação a serviços de computação em nuvem, sistemas de inteligência artificial, ferramentas de comunicação, softwares e infraestruturas digitais desenvolvidas por grandes empresas privadas transnacionais. Essa dependência pode gerar tensões entre a necessidade de fiscalização estatal e a utilização, pelo próprio Estado, de soluções fornecidas pelos agentes que integram o ecossistema econômico a ser regulado. Em tais circunstâncias, a capacidade regulatória não depende apenas da existência de normas jurídicas, mas também da autonomia tecnológica do poder público.⁴

Desse modo, a ANPD ocupa posição estratégica, mas seus desafios revelam os limites de uma proteção de dados fundada apenas na conformidade normativa. A autoridade é indispensável para a aplicação da LGPD, para a construção de uma cultura de proteção de dados e para a responsabilização de agentes de tratamento. No entanto, diante da concentração econômica, tecnológica e informacional das Big Techs, a fiscalização nacional enfrenta obstáculos que ultrapassam a dimensão administrativa. Regular a colonialidade de dados exige não apenas uma autoridade formalmente competente, mas também capacidade estatal de auditoria, infraestrutura técnica, cooperação institucional, transparência algorítmica e políticas públicas voltadas à soberania digital.

Assim, a análise da ANPD demonstra que a efetividade da LGPD depende de condições institucionais e materiais mais amplas. A proteção dos dados pessoais não se realiza apenas pela previsão abstrata de direitos, bases legais e sanções, mas pela existência de um Estado capaz de fiscalizar atores globais, compreender sistemas técnicos complexos e impor limites reais à exploração econômica da vida informacional. Essa constatação prepara a discussão seguinte, relativa aos fluxos transfronteiriços de dados e à dependência brasileira de infraestruturas digitais estrangeiras.

⁴ SERPRO, 2021; SERPRO, 2023.

3.4 Impactos na Soberania Nacional: Fluxo transfronteiriço e a dependência de servidores estrangeiros

A circulação internacional de dados pessoais constitui um dos principais desafios para a efetividade da Lei Geral de Proteção de Dados. Em uma economia digital estruturada por plataformas globais, serviços de computação em nuvem, cadeias internacionais de processamento e modelos de negócio baseados na extração massiva de informações, os dados raramente permanecem restritos ao território do Estado em que foram produzidos. Desse modo, a proteção jurídica dos titulares brasileiros depende não apenas da aplicação interna da LGPD, mas também da capacidade do país de exercer controle sobre fluxos informacionais que atravessam fronteiras e são frequentemente processados por agentes econômicos situados no exterior.⁵

A LGPD buscou enfrentar parcialmente esse problema ao estabelecer uma regra de aplicação extraterritorial. Nos termos do art. 3º, a lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou jurídica, de direito público ou privado, independentemente do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional, tenha por objetivo a oferta ou o fornecimento de bens ou serviços a indivíduos localizados no Brasil, ou envolva dados pessoais coletados no território nacional (BRASIL, 2018, art. 3º). Trata-se de mecanismo relevante, pois impede que agentes estrangeiros escapem automaticamente da legislação brasileira apenas por estarem formalmente sediados fora do país.

Além disso, a legislação disciplina a transferência internacional de dados pessoais nos arts. 33 a 36. O art. 33 prevê hipóteses nas quais a transferência internacional poderá ocorrer, como para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD, quando houver garantias contratuais específicas, cláusulas-padrão, normas corporativas globais, selos, certificados, cooperação jurídica internacional, execução de política pública, proteção da vida ou da incolumidade física, autorização da ANPD, consentimento específico do titular ou cumprimento de obrigação legal ou regulatória (BRASIL, 2018, arts. 33-36). Em tese, tais mecanismos procuram impedir que a circulação internacional de dados resulte na redução do nível de proteção assegurado aos titulares brasileiros.

Contudo, a existência dessas previsões normativas não elimina as dificuldades práticas de controle sobre os fluxos transfronteiriços. A circulação internacional de dados ocorre em

⁵ GOOGLE, 2026; MICROSOFT, 2026.

cadeias técnicas e contratuais complexas, envolvendo controladores, operadores, provedores de nuvem, data centers, redes de distribuição de conteúdo e prestadores de serviços localizados em diferentes jurisdições. Como observa Bioni, a fluidez dos dados pessoais e a multiplicidade de atores envolvidos no tratamento tornam o fluxo informacional difícil de determinar, o que compromete a possibilidade de controle efetivo pelo titular e desafia a própria atuação regulatória (BIONI, 2019, p. 26). Desse modo, o titular pode até ser formalmente informado sobre a transferência internacional, mas dificilmente possui condições reais de compreender para onde seus dados circulam, por quais agentes são tratados e quais padrões de proteção efetivamente incidem sobre essas operações.

Essa complexidade também afeta a capacidade fiscalizatória do Estado brasileiro. Ainda que a LGPD possua aplicação extraterritorial, a investigação e a responsabilização de agentes estrangeiros dependem de cooperação internacional, instrumentos administrativos eficazes, capacidade técnica da autoridade reguladora e mecanismos que permitam rastrear os fluxos reais de tratamento. Assim, a previsão normativa de incidência da lei não se confunde com a capacidade material de impor limites a corporações transnacionais que organizam suas operações de modo distribuído e tecnologicamente opaco.

Nesse ponto, a discussão ultrapassa a proteção individual da privacidade e alcança a soberania nacional. A soberania digital envolve a capacidade de um Estado definir regras, fiscalizar infraestruturas, controlar fluxos estratégicos de informação e preservar autonomia sobre dados relevantes para sua população, sua administração pública e seu desenvolvimento econômico. Quando os dados produzidos no território brasileiro são continuamente transferidos, armazenados, processados e monetizados por empresas estrangeiras, a questão deixa de ser apenas contratual ou consumerista e passa a envolver dependência tecnológica, assimetria regulatória e perda de capacidade decisória.

A dependência de infraestruturas digitais estrangeiras aprofunda esse problema. Serviços de nuvem, plataformas de comunicação, sistemas de inteligência artificial, ferramentas educacionais, soluções administrativas e ambientes de armazenamento frequentemente são fornecidos por grandes corporações transnacionais. Em muitos casos, mesmo quando o serviço é utilizado por instituições brasileiras, a infraestrutura técnica, os padrões contratuais, os códigos, os algoritmos e as políticas de governança permanecem sob controle de empresas sediadas em outros países. Essa situação limita a capacidade do Estado brasileiro de compreender, auditar e orientar integralmente o tratamento de dados estratégicos.

Esse quadro desloca a análise da mera licitude formal da transferência internacional para as condições materiais de sua governança. A autorização jurídica prevista na LGPD pode

assegurar um padrão normativo de proteção, mas não garante, por si só, que o Estado brasileiro consiga acompanhar tecnicamente as cadeias de tratamento, auditar infraestruturas estrangeiras ou impor limites efetivos a fluxos informacionais organizados por agentes privados transnacionais.

Nesse contexto, a LGPD apresenta uma limitação estrutural. Embora seus dispositivos sobre aplicação extraterritorial e transferência internacional sejam relevantes para proteger direitos dos titulares, eles não foram concebidos para enfrentar, sozinhos, a dependência brasileira de infraestruturas digitais estrangeiras. A lei regula hipóteses de circulação e impõe requisitos jurídicos ao tratamento, mas não cria, por si mesma, capacidade nacional de armazenamento, processamento, auditoria e desenvolvimento tecnológico. Por isso, a proteção de dados, quando dissociada de políticas públicas de soberania digital, pode acabar apenas disciplinando juridicamente fluxos informacionais que continuam submetidos a centros privados e estrangeiros de poder.

Dessa forma, os fluxos transfronteiriços de dados revelam uma das principais contradições da proteção de dados no Brasil. A LGPD afirma a incidência da legislação brasileira sobre determinadas operações internacionais e estabelece condições para a transferência de dados pessoais ao exterior. No entanto, a efetividade dessa proteção depende de fatores que ultrapassam a previsão normativa, como capacidade regulatória, infraestrutura técnica, cooperação internacional, transparência das cadeias de tratamento e autonomia tecnológica. Sem esses elementos, a circulação global de dados tende a preservar assimetrias entre os sujeitos e instituições que produzem informações e os agentes que dispõem dos meios técnicos para processá-las, interpretá-las e convertê-las em valor econômico.

3.5 Manifestações da colonialidade de dados no contexto brasileiro

As dinâmicas analisadas ao longo deste capítulo não permanecem restritas ao plano abstrato da regulação jurídica. No contexto brasileiro, a colonialidade de dados manifesta-se de maneira concreta em setores estratégicos da administração pública, especialmente quando serviços essenciais passam a depender de infraestruturas digitais controladas por grandes corporações transnacionais. Educação, saúde e Judiciário constituem exemplos relevantes de como a digitalização estatal, embora frequentemente apresentada como modernização administrativa, pode aprofundar relações de dependência tecnológica e informacional.

No campo da educação, essa dependência revela-se de forma expressiva. Sérgio Amadeu da Silveira observa que os dados do Sistema de Seleção Unificada (SiSU), responsável pelo ingresso de estudantes em instituições públicas de ensino superior, passaram

a ser processados na plataforma Microsoft Azure. Com isso, informações relativas ao desempenho escolar, renda familiar, participação em programas sociais e demais dados pessoais de candidatos passaram a integrar uma infraestrutura controlada por uma corporação estrangeira (SILVEIRA; CASSINO; SOUZA, 2021, p. 40). O problema não está apenas na utilização de uma solução tecnológica privada, mas no deslocamento de dados educacionais sensíveis para ambientes cuja governança técnica e econômica escapa ao controle pleno das instituições públicas brasileiras.

Essa dinâmica também se manifesta na adoção de serviços fornecidos por grandes plataformas digitais no cotidiano das universidades federais. O uso de ferramentas de e-mail institucional, armazenamento em nuvem, videoconferência e ambientes colaborativos fornecidos por Google e Microsoft tende a ser justificado pela gratuidade aparente, pela praticidade e pela redução imediata de custos administrativos. Entretanto, tais serviços não são neutros: eles inserem estudantes, docentes, pesquisadores e servidores em ecossistemas privados de produção, circulação e armazenamento de dados. Assim, a universidade pública, espaço historicamente associado à produção autônoma de conhecimento, passa a depender de infraestruturas informacionais controladas por empresas estrangeiras.

Na área da saúde, a questão assume contornos ainda mais sensíveis. A digitalização de serviços públicos, prontuários, registros de vacinação, bases de atendimento e sistemas de integração de informações sanitárias amplia a eficiência da gestão pública e pode facilitar o acesso da população a políticas de saúde. Contudo, dados de saúde possuem natureza especialmente sensível, nos termos da própria LGPD, pois revelam aspectos íntimos da vida dos cidadãos e podem ser utilizados para inferências sobre riscos, vulnerabilidades, hábitos e condições futuras (BRASIL, 2018, art. 5º, II). Quando esses dados são armazenados, processados ou integrados por meio de infraestruturas privadas de difícil auditoria, a proteção jurídica prevista pela LGPD torna-se insuficiente se não houver controle material sobre os sistemas que sustentam sua circulação.

Fenômeno semelhante pode ser observado no sistema de justiça. Nos últimos anos, tribunais brasileiros passaram a incorporar ferramentas de inteligência artificial, automação processual e soluções digitais voltadas à gestão de acervos, triagem de processos, elaboração de minutas e aumento da eficiência institucional, como demonstram iniciativas oficiais de IA aplicada à Justiça Federal (TRF1, 2024). Embora essas iniciativas sejam frequentemente apresentadas como instrumentos de modernização e celeridade, elas também revelam a crescente mediação tecnológica de atividades tradicionalmente associadas à soberania estatal. Quando dados judiciais, padrões decisórios, documentos processuais e fluxos administrativos

passam a depender de tecnologias cuja governança pode permanecer distante do controle público integral, a discussão deixa de ser apenas operacional e passa a envolver autonomia institucional, segurança informacional e controle democrático.

Nesse contexto, merece destaque a reflexão desenvolvida por Mariella Batarra Mian acerca da adoção crescente de plataformas privadas por instituições públicas brasileiras. Segundo a autora, a justificativa frequentemente apresentada para essas escolhas está associada aos princípios da eficiência e da economicidade, uma vez que soluções fornecidas por grandes empresas de tecnologia costumam demandar menos investimentos imediatos do que o desenvolvimento de infraestruturas próprias. Contudo, a aparente gratuidade ou vantagem econômica dessas plataformas integra precisamente seu modelo de negócio, baseado na obtenção contínua de dados produzidos por usuários e instituições públicas, convertendo a própria utilização dos serviços em fonte permanente de geração de valor para as Big Techs (MIAN, 2021, p. 129-133).

Sob essa perspectiva, a adesão de órgãos públicos a infraestruturas privadas estrangeiras não representa apenas uma decisão técnica ou financeira, mas também uma escolha política com impactos sobre a autonomia tecnológica nacional. Ao privilegiar soluções prontas desenvolvidas por corporações transnacionais, reduz-se o incentivo à construção de capacidades locais de desenvolvimento tecnológico, armazenamento público de dados, interoperabilidade entre sistemas nacionais e gestão soberana da informação. Aquilo que se apresenta como economicamente vantajoso no curto prazo pode, no longo prazo, aprofundar a dependência estrutural do país em relação a infraestruturas digitais controladas por agentes externos.

Essas manifestações demonstram que a colonialidade de dados não opera apenas pela coleta privada de informações de usuários em redes sociais ou plataformas de consumo. Ela também se realiza por meio da incorporação de infraestruturas digitais estrangeiras ao funcionamento cotidiano do Estado, das universidades, dos sistemas de saúde e do Poder Judiciário. Nesses casos, a materialidade da dependência aparece nos contratos de nuvem, nos servidores, nos softwares proprietários, nas plataformas educacionais, nos sistemas de IA, nas bases de dados e nos padrões técnicos que condicionam a circulação das informações públicas.

Essa tensão também pode ser observada no caso das empresas públicas de tecnologia. Gabriel Boscardim de Moraes, ao analisar a atuação do Serpro em relação às Big Techs, observa que a empresa ocupa posição estratégica na prestação de serviços de tecnologia da informação ao Estado brasileiro, justamente por lidar com dados e sistemas relevantes para a

administração pública federal. Contudo, o autor aponta que parcerias envolvendo o Serpro e grandes empresas de tecnologia, como Google, Microsoft, Amazon, Huawei, IBM e Oracle, revelam uma contradição entre a função soberana das empresas públicas de tecnologia e a crescente presença de agentes privados transnacionais na transformação digital do serviço público (BOSCARDIM DE MORAES, 2024, p. 67). Esse exemplo demonstra que a colonialidade de dados não se manifesta apenas na relação entre usuários e plataformas, mas também nas escolhas institucionais que definem quem controla a infraestrutura digital do próprio Estado.

Dessa forma, ainda que a LGPD estabeleça princípios relevantes de finalidade, necessidade, transparência, segurança e responsabilização, sua aplicação formal não elimina as bases materiais que estruturam a economia digital brasileira. A legislação pode regular o tratamento dos dados, mas não define, por si só, quem controla a infraestrutura, quem desenvolve os sistemas, quem audita os algoritmos e quem se apropria do valor produzido pelos fluxos informacionais. Por isso, as manifestações concretas da colonialidade de dados no Brasil revelam que a proteção jurídica dos titulares precisa ser articulada a uma política mais ampla de soberania digital, capaz de enfrentar não apenas abusos pontuais, mas também as condições estruturais que mantêm serviços públicos, instituições de ensino e órgãos estatais vinculados a plataformas e infraestruturas estrangeiras.

4 CAPÍTULO III - ESTRATÉGIAS DE DESCOLONIZAÇÃO E SOBERANIA DIGITAL

A análise desenvolvida nos capítulos anteriores demonstrou que os limites da Lei Geral de Proteção de Dados não decorrem apenas de falhas internas da legislação, mas de sua inserção em uma economia digital marcada pela concentração de infraestrutura, conhecimento técnico, capacidade computacional e poder econômico em grandes corporações transnacionais. Desse modo, enfrentar a colonialidade de dados exige ultrapassar a perspectiva da mera conformidade normativa e discutir estratégias capazes de fortalecer a autonomia informacional brasileira.

Nesse sentido, a soberania digital não deve ser compreendida como isolamento tecnológico ou rejeição abstrata das inovações digitais. Ao contrário, trata-se da capacidade de um Estado, de suas instituições e de sua sociedade definirem, de maneira democrática, os critérios de desenvolvimento, contratação, armazenamento, circulação, auditoria e utilização de tecnologias digitais. A questão central não é impedir a circulação internacional de dados ou a cooperação tecnológica, mas evitar que a digitalização do país ocorra em condições de dependência estrutural, baixa transparência e reduzida capacidade de controle público.

Este capítulo tem por objetivo discutir caminhos para a descolonização da tecnologia e o fortalecimento da soberania digital brasileira. Para isso, inicialmente será desenvolvido um diálogo com referências regulatórias internacionais, especialmente o Regulamento Geral de Proteção de Dados da União Europeia e a Personal Information Protection Law chinesa, com atenção aos diferentes modos pelos quais esses regimes articulam proteção de dados, controle de fluxos informacionais e capacidade regulatória estatal (UNIÃO EUROPEIA, 2016, arts. 3º, 44-46 e 83; CHINA, 2021, arts. 36, 38-40 e 66). Em seguida, será examinada a crítica hacker-fanoniana desenvolvida por Faustino e Lippold, a fim de pensar a tecnologia como campo de disputa política, econômica e epistemológica, e não como instrumento neutro ou inevitável. Por fim, serão apresentadas propostas voltadas à construção de uma política brasileira de soberania digital, envolvendo infraestrutura pública, armazenamento estratégico de dados, transparência algorítmica, interoperabilidade, fortalecimento institucional e educação digital crítica.

4.1 Referências regulatórias internacionais: PIPL chinesa e GDPR europeu como contrapontos à LGPD

O diálogo com referências regulatórias internacionais permite compreender que a regulação de informações pessoais não possui uma única orientação possível. Embora legislações contemporâneas compartilhem princípios como transparência, finalidade, necessidade, segurança e responsabilização, elas podem assumir funções distintas conforme o projeto político, econômico e institucional no qual estão inseridas. Nesse sentido, o Regulamento Geral de Proteção de Dados da União Europeia e a Personal Information Protection Law chinesa oferecem contrapontos relevantes para a análise dos limites da Lei Geral de Proteção de Dados brasileira.

O GDPR consolidou-se como uma das principais referências internacionais em matéria de proteção de dados pessoais. Sua estrutura normativa parte da centralidade dos direitos fundamentais, da proteção da privacidade e da responsabilização dos agentes de tratamento. O art. 3º do regulamento estabelece alcance territorial ampliado, aplicando-se ao tratamento realizado no contexto das atividades de controlador ou operador estabelecido na União Europeia, ainda que o tratamento ocorra fora do bloco. O mesmo dispositivo também alcança controladores ou operadores não estabelecidos na União Europeia quando as atividades de tratamento estiverem relacionadas à oferta de bens ou serviços a titulares localizados no território europeu ou ao monitoramento de seu comportamento (UNIÃO EUROPEIA, 2016, art. 3º). Essa previsão demonstra uma tentativa de impedir que empresas globais escapem da incidência regulatória apenas por se organizarem formalmente fora do território europeu.

Outro aspecto relevante do GDPR está na disciplina das transferências internacionais de dados. O art. 44 estabelece o princípio geral segundo o qual qualquer transferência de dados pessoais para país terceiro ou organização internacional deve observar as condições previstas no próprio regulamento, de modo que o nível de proteção assegurado às pessoas naturais não seja comprometido. O art. 45 prevê a possibilidade de transferência com base em decisão de adequação da Comissão Europeia, quando o país terceiro ou organismo internacional assegurar nível adequado de proteção. Já o art. 46 admite transferências mediante garantias apropriadas, como cláusulas contratuais-padrão, normas corporativas vinculantes, instrumentos jurídicos entre autoridades públicas e mecanismos de certificação (UNIÃO EUROPEIA, 2016, arts. 44-46). Dessa forma, a transferência internacional não é

tratada como simples operação contratual entre agentes privados, mas como prática condicionada à preservação de garantias jurídicas efetivas aos titulares.

O GDPR também se destaca por seu regime sancionatório. O art. 83 prevê multas administrativas que podem alcançar valores expressivos, inclusive percentuais calculados sobre o faturamento anual global da empresa infratora, conforme a natureza, gravidade e duração da infração, bem como o grau de responsabilidade do agente de tratamento (UNIÃO EUROPEIA, 2016, art. 83). Esse ponto é relevante para a análise brasileira porque evidencia que a proteção de dados, para ser efetiva diante de grandes corporações transnacionais, depende não apenas da previsão abstrata de direitos, mas de instrumentos institucionais capazes de impor custos reais ao descumprimento da legislação.

A LGPD brasileira foi fortemente influenciada por essa matriz europeia, especialmente no que se refere aos princípios de tratamento, aos direitos dos titulares, às bases legais e à disciplina da transferência internacional de dados. Contudo, a incorporação de elementos normativos semelhantes não gera, por si só, a mesma capacidade regulatória. A União Europeia atua como bloco econômico de grande peso geopolítico, possui autoridades de proteção de dados mais consolidadas e dispõe de maior capacidade de impor seus padrões a empresas globais. O Brasil, por sua vez, embora tenha criado uma legislação relevante, enfrenta limitações institucionais, econômicas e tecnológicas que reduzem sua capacidade de confrontar o poder das Big Techs.

A experiência chinesa apresenta uma orientação distinta, sendo especialmente relevante para a discussão sobre soberania digital. A Personal Information Protection Law, aprovada em 2021, também disciplina direitos dos titulares, consentimento, transparência, tratamento de dados sensíveis, decisões automatizadas e responsabilidade dos agentes de tratamento. Contudo, diferentemente de modelos centrados predominantemente na tutela individual da privacidade, a legislação chinesa articula a proteção de dados pessoais a uma estratégia mais ampla de controle estatal sobre fluxos informacionais, infraestrutura digital, segurança nacional e desenvolvimento tecnológico (CHINA, 2021, arts. 13-31 e 55-59). Por isso, sua relevância para esta pesquisa está em demonstrar que dados pessoais não são apenas objeto de proteção individual, mas também elementos estratégicos de soberania.

Um dos pontos mais expressivos da PIPL está na exigência de armazenamento territorial em determinadas hipóteses. O art. 36 determina que informações pessoais tratadas por órgãos estatais devem ser armazenadas no território continental chinês, admitindo fornecimento ao exterior apenas quando houver necessidade real e mediante avaliação de segurança. O art. 40, por sua vez, estabelece que operadores de infraestrutura crítica de

informação e agentes que tratem grandes volumes de dados pessoais devem armazenar internamente as informações coletadas e produzidas no território chinês, submetendo eventual transferência internacional a avaliação de segurança organizada pela autoridade competente (CHINA, 2021, arts. 36 e 40). Esses dispositivos revelam uma compreensão mais robusta da relação entre proteção de dados, infraestrutura e soberania nacional.

A PIPL também impõe requisitos específicos para a transferência internacional de dados pessoais. O art. 38 prevê que o envio de informações pessoais ao exterior depende do cumprimento de condições como aprovação em avaliação de segurança, certificação de proteção de informações pessoais, celebração de contrato com o destinatário estrangeiro conforme modelo definido pela autoridade competente, ou outras hipóteses previstas em lei. Além disso, o art. 39 exige que o titular seja informado sobre a identidade do destinatário estrangeiro, a finalidade, o método de tratamento, as categorias de dados transferidos e os meios para exercício de seus direitos, exigindo consentimento separado para essa transferência (CHINA, 2021, arts. 38 e 39). Assim, a circulação internacional de dados é tratada como tema estratégico, submetido não apenas à vontade individual do titular, mas também a mecanismos institucionais de controle e avaliação de risco.

Do ponto de vista sancionatório, a PIPL também prevê instrumentos relevantes. O art. 66 autoriza a imposição de medidas como correção de condutas, confisco de ganhos ilícitos, suspensão ou encerramento de serviços e multas elevadas, que podem alcançar montantes expressivos ou percentual da receita anual em casos graves, além da responsabilização de dirigentes e pessoas diretamente responsáveis (CHINA, 2021, art. 66). Esse desenho reforça a capacidade do Estado chinês de intervir sobre agentes econômicos que tratam dados em larga escala, demonstrando que a proteção de dados pode ser vinculada a mecanismos concretos de disciplina econômica e controle de fluxos informacionais.

O diálogo entre GDPR, PIPL e LGPD revela, portanto, três orientações distintas. O modelo europeu privilegia a proteção de direitos fundamentais, a responsabilização dos agentes de tratamento e a circulação internacional condicionada à manutenção de garantias equivalentes. O modelo chinês, por sua vez, confere maior centralidade à dimensão estratégica dos dados, articulando proteção individual, localização, segurança, controle de fluxos transfronteiriços e fortalecimento da capacidade regulatória estatal. O modelo brasileiro aproxima-se normativamente da matriz europeia, mas ainda carece de instrumentos materiais e institucionais capazes de enfrentar a dependência tecnológica e a concentração da infraestrutura digital.

Dessa forma, a análise dessas referências regulatórias permite compreender que o problema brasileiro não se resume à ausência de normas de proteção de dados. A LGPD possui princípios relevantes, reconhece direitos aos titulares, disciplina bases legais, prevê sanções administrativas e regula transferências internacionais. Contudo, diferentemente da União Europeia, o Brasil não dispõe do mesmo peso geopolítico e institucional para impor padrões globais às plataformas; e, diferentemente da China, ainda não estruturou uma política robusta de localização, controle estratégico de fluxos informacionais e desenvolvimento de infraestrutura própria. Essa posição intermediária contribui para que a proteção de dados no país permaneça juridicamente relevante, mas materialmente limitada.

A conclusão que se extrai dessa comparação não é a importação automática de um modelo estrangeiro, mas a necessidade de reconhecer que dados pessoais e infraestruturas digitais são temas de soberania. Nesse ponto, a experiência chinesa oferece uma contribuição importante ao demonstrar que a regulação de dados pode ser articulada a uma estratégia nacional de autonomia tecnológica e controle de fluxos informacionais. Para o Brasil, o desafio consiste em construir uma soberania digital democrática, capaz de combinar proteção de direitos fundamentais, fortalecimento da ANPD, controle de transferências internacionais, critérios rigorosos para contratação pública de tecnologias, incentivo à infraestrutura nacional e transparência algorítmica.

4.2 Crítica Hacker-Fanoniana: Descolonizando a tecnologia e a soberania algorítmica

As limitações identificadas ao longo deste trabalho demonstram que a superação da colonialidade de dados não depende exclusivamente do aperfeiçoamento da legislação de proteção de dados pessoais. Reformas normativas são indispensáveis, especialmente para fortalecer a transparência, a fiscalização e o controle sobre fluxos internacionais de dados. Contudo, elas não são suficientes para enfrentar estruturas históricas de dependência tecnológica e epistemológica construídas ao longo da consolidação da economia digital. A construção de uma efetiva soberania digital exige também disputar os sentidos da tecnologia, seus modos de produção, seus critérios de funcionamento e os sujeitos autorizados a desenvolvê-la e controlá-la.

Nesse ponto, a crítica hacker-fanoniana desenvolvida por Deivison Faustino e Walter Lippold oferece uma contribuição relevante. Para os autores, o colonialismo digital não deve ser compreendido apenas como problema de acesso desigual a tecnologias, mas como expressão contemporânea de relações de exploração, racialização, dependência e controle inscritas no próprio desenvolvimento capitalista das forças produtivas (FAUSTINO;

LIPPOLD, 2023, p. 22-23). A tecnologia, portanto, não aparece como instrumento neutro, situado fora da história, mas como forma social atravessada por interesses econômicos, disputas geopolíticas, relações de classe e hierarquias coloniais.

Essa leitura permite romper com o chamado fetiche da tecnologia, isto é, com a tendência de tratar sistemas digitais, plataformas, algoritmos e inteligências artificiais como soluções naturalmente eficientes, inevitáveis ou emancipadoras. A crítica hacker-fanoniana evidencia que a tecnologia pode ampliar capacidades humanas e sociais, mas também pode intensificar a exploração, a vigilância, a dependência e a concentração de poder. Assim, o problema não está na existência da técnica em si, mas nas condições políticas, econômicas e sociais que determinam sua produção, sua propriedade, sua finalidade e sua apropriação.

A contribuição de Frantz Fanon é fundamental para essa reflexão. Ao analisar os processos de descolonização, Fanon demonstra que a superação do colonialismo não se realiza apenas pela substituição formal dos sujeitos que ocupam o poder, mas pela transformação profunda das estruturas materiais, culturais e subjetivas herdadas da dominação colonial (FANON, 2022, p. 31-33). No campo tecnológico, essa perspectiva impede que a soberania digital seja reduzida à simples adoção de ferramentas modernas por países periféricos. Uma tecnologia produzida a partir de interesses externos, padrões proprietários fechados e infraestruturas dependentes pode reproduzir relações coloniais mesmo quando utilizada por instituições nacionais.

Faustino e Lippold recuperam, nesse sentido, a experiência analisada por Fanon acerca do uso do rádio na Revolução Argelina. O rádio, inicialmente associado à presença colonial francesa e à difusão de discursos do colonizador, foi reapropriado pelos revolucionários argelinos como instrumento de comunicação, organização e resistência política. Esse exemplo revela que a tecnologia não possui sentido fixo ou destino inevitável: seu significado depende das relações sociais e políticas nas quais é inserida. Um aparato técnico pode servir à dominação colonial, mas também pode ser reconfigurado como ferramenta de luta, desde que apropriado por sujeitos coletivos capazes de transformá-lo em instrumento de emancipação (FAUSTINO; LIPPOLD, 2023, p. 181-182).

A partir dessa chave, descolonizar a tecnologia não significa rejeitar a inovação, defender isolamento técnico ou retornar a um passado pré-digital. Significa questionar quem define as finalidades dos sistemas tecnológicos, quem controla suas infraestruturas, quem audita seus algoritmos, quem se beneficia da extração de dados e quais formas de vida são favorecidas ou marginalizadas por suas operações. A crítica hacker-fanoniana desloca a

discussão da mera utilização de tecnologias para a disputa sobre sua arquitetura, sua governança e seus efeitos sociais.

Esse ponto é especialmente relevante diante da ascensão da inteligência artificial e dos sistemas algorítmicos de decisão. Algoritmos não apenas processam informações, mas classificam sujeitos, organizam visibilidades, hierarquizam possibilidades e influenciam decisões em áreas como consumo, trabalho, crédito, educação, segurança pública, saúde e justiça. Quando esses sistemas são desenvolvidos, treinados e controlados por grandes corporações transnacionais, a dependência tecnológica não se limita ao uso de ferramentas estrangeiras, mas alcança a própria produção dos critérios pelos quais a realidade social passa a ser interpretada e administrada.

Nesse contexto, a noção de soberania algorítmica torna-se central. Ela pode ser compreendida como a capacidade de um Estado e de sua sociedade compreenderem, desenvolverem, auditarem e orientarem sistemas algorítmicos de acordo com finalidades públicas, democráticas e coletivas. Não se trata apenas de possuir servidores ou armazenar dados em território nacional, embora esses elementos sejam relevantes. Trata-se também de construir capacidade técnica, científica e institucional para questionar modelos automatizados, exigir explicabilidade, identificar vieses, controlar finalidades de tratamento e impedir que decisões socialmente relevantes sejam delegadas a sistemas opacos e orientados por interesses privados.

A soberania algorítmica também possui dimensão epistemológica. Como observa Paola Ricaurte, a racionalidade centrada em dados tende a apresentar-se como forma superior e objetiva de conhecimento, deslegitimando outras maneiras de compreender e organizar a vida social (RICAURTE, 2019, p. 352-354). Sob essa perspectiva, a dependência tecnológica não envolve apenas infraestrutura e mercado, mas também a imposição de modelos de conhecimento produzidos por centros hegemônicos. Descolonizar a tecnologia exige, portanto, reconhecer a pluralidade de saberes, necessidades e experiências que devem orientar o desenvolvimento tecnológico, especialmente em sociedades marcadas por desigualdades raciais, territoriais, econômicas e culturais.

Essa perspectiva aproxima a crítica hacker-fanoniana da discussão jurídica sobre proteção de dados. A LGPD é indispensável para estabelecer direitos, princípios e deveres no tratamento de informações pessoais, mas sua aplicação formal não enfrenta, sozinha, a alienação técnica que separa os titulares, as instituições públicas e a sociedade dos sistemas que organizam a vida digital. Quando os indivíduos são reduzidos à condição de usuários de plataformas fechadas, e o Estado à condição de contratante de soluções prontas, a soberania

digital permanece limitada. A proteção de dados precisa ser acompanhada de capacidade pública de compreensão, desenvolvimento, auditoria e controle social das tecnologias.

Dessa forma, a crítica hacker-fanoniana permite compreender que a superação da colonialidade de dados passa por uma disputa política sobre a tecnologia. Não basta regular juridicamente a extração de dados se os meios técnicos de coleta, armazenamento, processamento e interpretação permanecerem concentrados em corporações transnacionais. Também não basta ampliar o acesso a ferramentas digitais se esse acesso ocorrer em condições de dependência, opacidade e submissão a padrões proprietários. A descolonização tecnológica exige reapropriação crítica, formação técnica, desenvolvimento de infraestruturas públicas, fortalecimento de comunidades tecnológicas locais e construção de modelos de governança orientados pelo interesse público.

Em última análise, a soberania algorítmica não constitui um fim em si mesma, mas um instrumento para que o desenvolvimento tecnológico possa ser orientado pelos interesses sociais, democráticos e emancipatórios das próprias comunidades. A partir da crítica hacker-fanoniana, a tecnologia deixa de ser compreendida como destino inevitável e passa a ser tratada como campo de luta. Essa compreensão prepara a discussão seguinte, voltada à formulação de propostas concretas para o fortalecimento da soberania digital brasileira.

4.3 Propostas para a soberania digital brasileira: Nuvem pública nacional, armazenamento local de dados sensíveis e educação digital

A análise desenvolvida ao longo deste trabalho permite afirmar que a proteção de dados pessoais, embora indispensável, não é suficiente para enfrentar a colonialidade de dados no Brasil. A LGPD representa avanço normativo relevante ao reconhecer direitos dos titulares, estabelecer princípios de tratamento e criar mecanismos de responsabilização dos agentes públicos e privados. Contudo, como demonstrado nos capítulos anteriores, a eficácia da legislação permanece limitada quando os meios técnicos de coleta, armazenamento, processamento e interpretação dos dados continuam concentrados em grandes corporações transnacionais. Por isso, a construção de uma política de soberania digital deve articular proteção jurídica, infraestrutura tecnológica, capacidade estatal, transparência algorítmica e educação crítica.

Um primeiro caminho consiste no fortalecimento da infraestrutura pública de dados, especialmente por meio de empresas públicas de tecnologia. A soberania digital exige que o Estado brasileiro possua capacidade própria de armazenamento, processamento e gestão de informações estratégicas, sobretudo aquelas vinculadas a políticas públicas, saúde, educação,

segurança, justiça, assistência social, tributação e administração governamental. Nesse ponto, a atuação de empresas como Serpro e Dataprev deve ser compreendida não apenas como prestação técnica de serviços digitais, mas como instrumento de manutenção da soberania nacional. Como observa Boscardim de Moraes, empresas públicas podem desempenhar papel relevante na redução da dependência em relação a agentes privados estrangeiros, na preservação de dados estratégicos e na construção de capacidades tecnológicas internas (BOSCARDIM DE MORAES, 2024, p. 71-74).

O fortalecimento dessas empresas, porém, não pode ser compreendido apenas como ampliação formal de sua atuação. É necessário assegurar que sua governança esteja efetivamente orientada pelo interesse público, pela segurança nacional, pela soberania de dados e pela redução da dependência tecnológica. O caso do Serpro demonstra essa ambivalência: embora a empresa possua função estratégica no processamento de dados e na prestação de serviços de tecnologia da informação ao Estado brasileiro, suas parcerias com grandes empresas de tecnologia para oferta de serviços de nuvem revelam o risco de que a infraestrutura pública funcione como porta de entrada para a ampliação da presença das Big Techs na transformação digital do serviço público (BOSCARDIM DE MORAES, 2024, p. 71-74). Assim, empresas públicas de tecnologia só contribuem plenamente para a soberania digital quando atuam como instrumentos de autonomia estatal, e não como intermediárias da dependência em relação a fornecedores privados transnacionais.

Outro eixo indispensável envolve a definição de critérios mais rigorosos para a contratação pública de tecnologias digitais. Órgãos públicos não devem avaliar plataformas, softwares e serviços de nuvem apenas a partir de critérios imediatos de preço, eficiência ou praticidade. Também devem ser considerados fatores como localização dos dados, auditabilidade dos sistemas, transparência sobre fluxos informacionais, portabilidade, reversibilidade contratual, interoperabilidade, uso de padrões abertos, prevenção de dependência exclusiva em relação a fornecedores privados, segurança da informação e compatibilidade com finalidades públicas. A economicidade, quando isolada de uma análise sobre soberania, pode justificar escolhas aparentemente vantajosas no curto prazo, mas capazes de aprofundar a dependência tecnológica no longo prazo.

A contratação pública deve ser tratada, portanto, como instrumento de política tecnológica. A escolha de serviços digitais pelo Estado define não apenas custos administrativos, mas também quais infraestruturas serão fortalecidas, quais padrões técnicos serão adotados, quais fornecedores passarão a controlar sistemas públicos e quais capacidades serão desenvolvidas internamente. Por isso, iniciativas como nuvens governamentais, regras

de contratação de serviços de nuvem e políticas de cibersegurança precisam estar articuladas a uma estratégia mais ampla de autonomia informacional. Sem essa articulação, mesmo projetos voltados à modernização digital podem reproduzir a dependência de plataformas estrangeiras e limitar a capacidade pública de controle sobre dados estratégicos.

Outra medida relevante consiste na adoção de regras específicas para dados estratégicos e sensíveis. A experiência comparada demonstra que determinados tipos de informação não podem ser tratados apenas como ativos privados ou objetos de relações contratuais. Dados de saúde, educação, justiça, segurança pública, biometria, infraestrutura crítica e administração estatal possuem relevância coletiva e estratégica. Por isso, o Brasil deve discutir critérios mais rigorosos para sua transferência internacional, armazenamento, compartilhamento e processamento, inclusive com exigências de avaliação de risco, auditoria independente e, em determinadas hipóteses, armazenamento em território nacional. Essa proposta não implica isolamento informacional, mas reconhecimento de que certos dados possuem impacto direto sobre a soberania nacional e os direitos fundamentais.

A soberania digital também exige o fortalecimento institucional da Autoridade Nacional de Proteção de Dados. A ANPD ocupa papel central na implementação da LGPD, mas sua atuação precisa ser acompanhada de condições materiais adequadas para fiscalizar agentes econômicos de grande porte. Isso envolve ampliação de capacidade técnica, equipes especializadas, instrumentos de auditoria, cooperação com universidades e centros de pesquisa, articulação com órgãos de defesa do consumidor, Ministério Público, Tribunal de Contas e entidades da sociedade civil. Diante de plataformas globais, a autoridade reguladora não pode atuar apenas de forma orientativa ou reativa, devendo possuir condições efetivas para investigar fluxos complexos de tratamento, decisões automatizadas, práticas de compartilhamento e modelos de negócio baseados na extração massiva de dados.

A transparência algorítmica constitui outra dimensão indispensável. Sistemas automatizados de decisão, inteligência artificial e mecanismos de recomendação não devem permanecer protegidos integralmente por sigilo empresarial quando produzem efeitos relevantes sobre direitos, oportunidades e acesso a serviços. É necessário estabelecer deveres de explicabilidade, avaliação de impacto, auditoria independente e prestação de contas, especialmente quando tais sistemas forem utilizados pelo poder público ou afetarem significativamente titulares de dados. A opacidade algorítmica dificulta o exercício da autodeterminação informacional e impede que a sociedade compreenda como dados pessoais são utilizados para classificar, prever, influenciar ou limitar comportamentos.

Além disso, o desenvolvimento de software livre, tecnologias abertas e comunidades técnicas nacionais deve ser tratado como parte de uma estratégia de soberania digital. A dependência de plataformas proprietárias estrangeiras reduz a capacidade de adaptação, fiscalização e controle dos sistemas utilizados por instituições públicas. O incentivo a soluções abertas, auditáveis e desenvolvidas localmente pode ampliar a autonomia tecnológica, estimular a inovação nacional, fortalecer universidades e centros públicos de pesquisa e permitir maior controle social sobre infraestruturas digitais. Essa diretriz aproxima-se da crítica hacker-fanoniana, pois compreende a tecnologia como campo de disputa e reapropriação coletiva, e não como produto fechado a ser consumido passivamente (FAUSTINO; LIPPOLD, 2023, p. 22-23).

A educação digital crítica também ocupa lugar central nesse processo. A proteção de dados não pode depender apenas da leitura individual de termos de uso ou da manifestação formal de consentimento. É necessário formar cidadãos, servidores públicos, estudantes, profissionais do direito e gestores para compreenderem os riscos da economia de dados, a lógica das plataformas, os limites do consentimento, a importância da segurança da informação e os impactos sociais da inteligência artificial. Essa educação não deve ser reduzida ao uso instrumental de ferramentas digitais, mas deve envolver reflexão sobre poder, privacidade, colonialidade, dependência tecnológica e direitos fundamentais.

Dessa forma, o enfrentamento da colonialidade de dados no Brasil exige uma política integrada, capaz de combinar LGPD, fortalecimento institucional, infraestrutura pública, controle de fluxos internacionais, transparência algorítmica, educação digital e desenvolvimento tecnológico nacional. A questão não é negar a importância da legislação existente, mas reconhecer que ela precisa ser inserida em um projeto mais amplo de autonomia informacional. Somente assim será possível deslocar a proteção de dados de uma lógica predominantemente formal de conformidade para uma estratégia democrática de controle social, desenvolvimento soberano e resistência às novas formas de dependência digital.

5 CONCLUSÃO

A presente pesquisa teve como objetivo analisar se a Lei Geral de Proteção de Dados é suficiente para enfrentar a colonialidade de dados no Brasil, especialmente diante da atuação das grandes plataformas digitais transnacionais e da dependência brasileira em relação a infraestruturas tecnológicas estrangeiras. Partiu-se da hipótese de que a LGPD, embora represente avanço normativo relevante, não é capaz, por si só, de conter práticas extrativistas baseadas na coleta, no processamento e na monetização massiva de dados pessoais, sobretudo quando tais práticas estão inseridas em uma economia digital marcada pela concentração de poder econômico, técnico e informacional nas Big Techs.

Ao longo do trabalho, verificou-se que o colonialismo de dados não pode ser compreendido apenas como violação pontual de privacidade ou como uso abusivo de informações pessoais. Trata-se de uma dinâmica estrutural de apropriação da vida social, pela qual comportamentos, relações, preferências, deslocamentos, interações e experiências cotidianas são convertidos em dados economicamente exploráveis. Nesse contexto, os dados pessoais deixam de ser simples registros informacionais e passam a integrar uma cadeia global de produção de valor, sustentada por plataformas digitais, infraestruturas de nuvem, sistemas algorítmicos, inteligência artificial e mercados de predição comportamental.

Essa constatação desloca a análise da proteção de dados para além da relação individual entre titular e controlador. Embora a LGPD reconheça direitos, estabeleça princípios e crie mecanismos de responsabilização, sua aplicação ocorre em um ambiente profundamente assimétrico. O titular formalmente protegido pela lei é, muitas vezes, o mesmo sujeito que depende de plataformas digitais para trabalhar, estudar, consumir, comunicar-se e acessar serviços públicos. Diante de contratos de adesão, políticas de privacidade complexas, opacidade algorítmica e infraestruturas técnicas inacessíveis, a autodeterminação informacional tende a operar mais como promessa normativa do que como poder efetivo de controle.

Nesse sentido, a insuficiência da LGPD não decorre apenas de lacunas internas da legislação. O problema é mais profundo: a proteção jurídica dos dados pessoais está inserida em uma economia digital cuja lógica depende da coleta contínua, do cruzamento massivo, da inferência comportamental e da conversão da experiência humana em valor econômico. A lei pode limitar abusos, exigir bases legais, impor deveres de transparência e reconhecer direitos aos titulares, mas não altera, sozinha, as condições materiais que sustentam a extração e a concentração dos dados. Por isso, a crítica desenvolvida neste trabalho não nega a importância

da LGPD, mas questiona sua suficiência diante de uma estrutura econômica e tecnológica globalmente desigual.

A análise também demonstrou que a colonialidade de dados possui dimensão material. A chamada “nuvem” não é espaço imaterial ou neutro, mas infraestrutura composta por cabos submarinos, data centers, servidores, energia, água, minerais, softwares, contratos e regimes de propriedade. O controle desses elementos define quem armazena, processa, interpreta e monetiza os dados produzidos socialmente. Quando países como o Brasil dependem de plataformas, serviços de nuvem e sistemas proprietários estrangeiros para executar funções públicas e privadas essenciais, a proteção de dados deixa de ser apenas tema de privacidade e passa a envolver soberania nacional, autonomia tecnológica e capacidade estatal.

Essa dimensão aparece de forma concreta no contexto brasileiro. A presença de grandes plataformas na educação, na administração pública, em serviços digitais, em universidades, em sistemas de nuvem e em empresas públicas de tecnologia revela que a colonialidade de dados não se limita à relação entre usuários e redes sociais. Ela também se manifesta nas escolhas institucionais que definem quais infraestruturas serão utilizadas, quais fornecedores serão fortalecidos, quais padrões técnicos serão adotados e quem terá capacidade de auditar, controlar e orientar os fluxos informacionais produzidos no país. A modernização digital, quando guiada apenas por critérios imediatos de eficiência, praticidade ou economicidade, pode aprofundar formas de dependência que permanecem ocultas sob a aparência de inovação.

O diálogo com diferentes regimes de proteção de dados reforçou essa conclusão. O modelo europeu demonstra a relevância de uma estrutura robusta de direitos fundamentais, responsabilização e controle de transferências internacionais. A experiência chinesa, por sua vez, evidencia que dados pessoais e infraestruturas digitais também podem ser tratados como elementos estratégicos de soberania, articulando proteção individual, localização, segurança nacional e controle de fluxos informacionais. O Brasil, embora tenha incorporado elementos relevantes da matriz europeia, ainda carece de instrumentos materiais, institucionais e tecnológicos capazes de enfrentar a dependência estrutural em relação às Big Techs.

Por isso, confirmou-se a hipótese central da pesquisa: a LGPD é necessária, mas insuficiente para enfrentar a colonialidade de dados no Brasil. Necessária, porque estabelece um marco jurídico indispensável para a proteção dos titulares, para a responsabilização dos agentes de tratamento e para a construção de uma cultura de proteção de dados. Insuficiente, porque não enfrenta, de maneira isolada, a concentração da infraestrutura digital, a opacidade algorítmica, a fragilidade da fiscalização, a dependência tecnológica, os fluxos

transfronteiriços de dados e os modelos de negócio baseados na extração massiva da vida informacional.

A resposta a esse problema não está na rejeição da tecnologia nem no isolamento informacional do país. A crítica ao colonialismo de dados não implica negar a inovação, mas disputar suas finalidades, seus meios e suas condições de apropriação. A tecnologia não é neutra: pode servir à ampliação de direitos, à democratização do conhecimento e à melhoria de serviços públicos, mas também pode aprofundar vigilância, dependência e concentração de poder. Descolonizar a tecnologia significa, portanto, construir capacidade social e estatal para compreender, desenvolver, auditar e orientar sistemas digitais conforme finalidades públicas, democráticas e emancipadoras.

Nesse horizonte, a soberania digital brasileira deve ser compreendida como projeto jurídico, político, econômico e tecnológico. A proteção de dados precisa ser articulada ao fortalecimento da ANPD, à transparência algorítmica, ao controle de fluxos internacionais, à regulação da contratação pública de tecnologias, ao desenvolvimento de infraestrutura pública, ao incentivo a software livre e padrões abertos, à proteção de dados estratégicos e à educação digital crítica. Além disso, exige integração entre regulação, política industrial, pesquisa pública, empresas estatais estratégicas, universidades, centros de inovação, formação técnica e participação social.

Conclui-se, portanto, que o enfrentamento da colonialidade de dados no Brasil exige deslocar a proteção de dados de uma lógica predominantemente formal de conformidade para uma estratégia ampla de soberania digital democrática. A LGPD deve ser preservada, fortalecida e aprofundada, mas inserida em um projeto nacional de autonomia tecnológica e controle social sobre a economia digital. Somente assim será possível transformar a proteção de dados pessoais em instrumento efetivo de defesa dos direitos fundamentais, da soberania nacional e da emancipação diante das novas formas de dependência digital.

REFERÊNCIAS

BADSHAH, Nadeem. Meta plans to link US and India with world's longest undersea cable project. **The Guardian**, 17 fev. 2025. Disponível em: <https://www.theguardian.com/technology/2025/feb/17/meta-plans-to-build-worlds-longest-underwater-sub-sea-cable-venture>. Acesso em: 2 jul. 2026.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BOSCARDIM DE MORAES, Gabriel. Empresas públicas para a soberania nacional: o caso do Serpro com as Big Techs e outras possibilidades. **ÂNDÉ: Ciências e Humanidades**, São Bernardo do Campo (SP), v. 8, n. 1, p. 065-080, 2024. DOI: 10.36942/iande.v8i1.985. Disponível em: <https://periodicos.ufabc.edu.br/index.php/iande/article/view/985>. Acesso em: 30 jun. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 30 jun. 2026.

BRASIL. **Lei nº 14.460, de 25 de outubro de 2022**. Transforma a Autoridade Nacional de Proteção de Dados em autarquia de natureza especial e transforma cargos em comissão. Brasília, DF: Presidência da República, 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/114460.htm. Acesso em: 30 jun. 2026.

CHINA. **Personal Information Protection Law of the People's Republic of China**. 2021. Tradução em inglês por DigiChina, Stanford Cyber Policy Center. Disponível em: <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/>. Acesso em: 30 jun. 2026.

COULDRY, Nick; MEJIAS, Ulises A. Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject. **Television & New Media**, v. 20, n. 4, p. 336-349, 2019a. DOI: 10.1177/1527476418796632.

COULDRY, Nick; MEJIAS, Ulises A. **The Costs of Connection: how data is colonizing human life and appropriating it for capitalism**. Stanford: Stanford University Press, 2019b.

FANON, Frantz. **Os condenados da terra**. Rio de Janeiro: Zahar, 2022.

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

GOOGLE. Política de Privacidade do Google. Em vigor a partir de 2 abr. 2026. Disponível em: <https://policies.google.com/privacy?hl=pt-BR>. Acesso em: 2 jul. 2026.

GROSGOUEL, Ramón. A estrutura do conhecimento nas universidades ocidentalizadas: racismo/sexismo epistêmico e os quatro genocídios/epistemicídios do longo século XVI. **Sociedade e Estado**, Brasília, v. 31, n. 1, p. 25-49, jan./abr. 2016. DOI: 10.1590/S0102-69922016000100003.

LÊNIN, Vladimir Ilitch. **O imperialismo, etapa superior do capitalismo**. São Paulo: Boitempo, 2021.

MARTINS, Laís; AMORIM, Francisco. TikTok construirá mega data center em cidade com histórico de seca no Ceará. **The Intercept Brasil**, 22 maio 2025. Disponível em: <https://www.intercept.com.br/2025/05/22/tiktok-data-center-cidade-seca-no-ceara/>. Acesso em: 30 jun. 2026.

MICROSOFT. Política de Privacidade da Microsoft. 2026. Disponível em: <https://www.microsoft.com/pt-br/privacy/privacystatement>. Acesso em: 2 jul. 2026.

MIAN, Mariella Batarra. Universidades Federais brasileiras a serviço da lógica colonial de exploração de dados. In: SILVEIRA, Sérgio Amadeu da; CASSINO, João Francisco; SOUZA, Joyce (org.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. São Paulo: Autonomia Literária, 2021.

MURPHY, Andrea; TUCKER, Hank. The Global 2000 2025. **Forbes**, 12 jun. 2025. Disponível em: <https://www.forbes.com/lists/global2000/>. Acesso em: 2 jul. 2026.

QUIJANO, Aníbal. Colonialidade do poder e classificação social. In: SANTOS, Boaventura de Sousa; MENESES, Maria Paula (org.). **Epistemologias do Sul**. Coimbra: Almedina, 2009. p. 73-118.

RICAURTE, Paola. Data Epistemologies, Coloniality of Power, and Resistance. **Television & New Media**, v. 20, n. 4, p. 350-365, 2019. DOI: 10.1177/1527476419831640.

SERPRO. Serviço em Nuvem do Serpro é reconhecido pela Amazon Web Services. **Serpro**, 20 out. 2021. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2021/cloud-serpro-selo-amazon>. Acesso em: 2 jul. 2026.

SERPRO. Serpro inaugura era de soberania digital em serviços de nuvem com o lançamento da Nuvem de Governo. **Serpro**, 28 nov. 2023. Disponível em: <https://www.serpro.gov.br/menu/noticias/noticias-2023/serpro-lanca-nuvem-de-governo>. Acesso em: 2 jul. 2026.

SILVEIRA, Sérgio Amadeu da; CASSINO, João Francisco; SOUZA, Joyce (org.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. São Paulo: Autonomia Literária, 2021.

TRIBUNAL REGIONAL FEDERAL DA 1ª REGIÃO. SJDF lança projeto de Inteligência Artificial que promete mais agilidade na tramitação processual. **TRF1**, 16 dez. 2024. Disponível em: <https://www.trf1.jus.br/trf1/noticias/sjdf-lanca-projeto-de-inteligencia-artificial-que-promete-mais-agilidade-na-tramitacao-processual->. Acesso em: 30 jun. 2026.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Jornal Oficial da União Europeia**, L 119, p. 1-88, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 30 jun. 2026.

WEATHERBED, Jess. Meta is building the “mother of all” subsea cables. **The Verge**, 29 nov. 2024. Disponível em: <https://www.theverge.com/2024/11/29/24308746/meta-10-billion-global-subsea-cable-project>. Acesso em: 2 jul. 2026.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Rio de Janeiro: Intrínseca, 2021.