Revista Brasileira de Filosofia e História-RBFH
Grupo Verde de Agroecologia e Abelhas-GVAA
ISSN: 2447-5076

Artigo

Entre a tutela de dados pessoais e a concentração de poder das Big Techs na mineração de criptomoedas

Between the guardianship of personal data and the concentration of power of Big Techs in cryptocurrency mining

Boanerges Alves da Costa Neto[1]

[1]Doutorando em Ciências Jurídicas pela Universidad do Museo Social Argentino, Buenos Aires. ORCID: 0009-0006-7592-1818. E-mail: bcadvogado@hotmail.com.

Submetido em: 12/04/2026, revisado em: 15/04/2026 e aceito para publicação em: 20/04/2026.

RESUMO: O presente artigo tem como base o cenário em que a economia de dados, a expansão das *big techs* no Brasil e a crescente digitalização de atividades econômicas, inclusive da mineração de criptomoedas, recolocam em evidência a capacidade do direito de limitar formas assimétricas de exercício de poder econômico, informacional e infraestrutural. Diante disso, a LGPD surgiu como resposta normativa a esse ambiente, prometendo reequilibrar a relação entre titulares e agentes de tratamento, ao mesmo tempo em que grandes plataformas estruturam modelos de negócio ancorados em coleta massiva, perfilização e integração de bases. À luz dessa questão, o estudo tem como objetivo analisar em que medida a LGPD atua, na prática, como obstáculo ao poder das *big techs* ou se acaba sendo apropriada como instrumento que legitima e consolida posições dominantes no ecossistema digital brasileiro, com atenção também ao modo como essas dinâmicas alcançam a mineração de criptomoedas, atividade cada vez mais dependente de infraestruturas digitais, serviços de nuvem, sistemas de identificação, monitoramento e circulação de dados. Para tanto, este trabalho desenvolve pesquisa qualitativa, jurídico-teórica e documental, por meio de leitura dogmática da Constituição, da LGPD, do Marco Civil da Internet, de atos normativos da ANPD e de decisões selecionadas do STF, STJ, CADE e da própria Autoridade Nacional. As discussões desenvolvidas deixam claro que programas de conformidade em proteção de dados podem impor custos elevados e funcionar como barreiras para agentes menores, inclusive em setores digitais emergentes. Porém, também mostram limites de fiscalização, transparência algorítmica e coordenação institucional, capazes de manter zonas de opacidade em torno das práticas das *big techs* e de atividades economicamente dependentes de suas infraestruturas, como a mineração de criptomoedas. Ao problematizar essas duas dimensões, o trabalho defende que a LGPD permanece em disputa, podendo fortalecer a tutela de direitos e conter abusos, entretanto, também pode ser absorvida como linguagem de legitimidade regulatória por atores que já concentram tecnologia, dados e capacidade de mercado.
Palavras-chave: Direitos Fundamentais; Proteção de Dados Pessoais; Big Techs; Regulação Digital; Governança de Dados; Mineração de Criptomoedas.

ABSTRACT: This article is grounded in a context in which the data economy, the expansion of big tech companies in Brazil, and the increasing digitalization of economic activities—including cryptocurrency mining—bring renewed attention to the capacity of law to limit asymmetric forms of economic, informational, and infrastructural power. In this setting, the Brazilian General Data Protection Law (LGPD) emerged as a normative response, aiming to rebalance the relationship between data subjects and data controllers, while large platforms continue to structure business models based on massive data collection, profiling, and database integration. In light of this issue, the study aims to analyze the extent to which the LGPD operates, in practice, as a constraint on the power of big tech companies, or whether it is ultimately appropriated as an instrument that legitimizes and consolidates dominant positions within the Brazilian digital ecosystem. Particular attention is given to how these dynamics extend to cryptocurrency mining, an activity increasingly dependent on digital infrastructures, cloud services, identification systems, monitoring mechanisms, and data flows. To this end, the research adopts a qualitative, legal-theoretical, and documentary approach, based on a doctrinal reading of the Constitution, the LGPD, the Brazilian Internet Civil Framework, regulatory acts issued by the National Data Protection Authority (ANPD), and selected decisions from the Federal Supreme Court (STF), the Superior Court of Justice (STJ), the Administrative Council for Economic Defense (CADE), and the Authority itself. The discussions developed indicate that data protection compliance programs may impose high costs and operate as barriers to entry for smaller actors, including those in emerging digital sectors. At the same time, they reveal limitations in enforcement, algorithmic transparency, and institutional coordination, which contribute to maintaining zones of opacity around the practices of big tech companies and of economic activities dependent on their infrastructures, such as cryptocurrency mining. By addressing these two dimensions, the study argues that the LGPD remains a contested field: it may strengthen the protection of rights and curb abuses, yet it can also be absorbed as a language of regulatory legitimacy by actors that already concentrate technological capacity, data control, and market power.
Keywords: Fundamental Rights; Personal Data Protection; Big Techs; Digital Regulation; Data Governance; Cryptocurrency Mining.

1 CONSIDERAÇÕES INICIAIS

A materialização da economia de dados e a expansão das *big techs* no território brasileiro recolocam em debate a capacidade do ordenamento jurídico de limitar formas assimétricas de exercício de poder econômico, informacional e político. Diante disso, a proteção de dados pessoais se tornou um eixo necessário da regulação das plataformas digitais, em diálogo com temas como livre concorrência, defesa do consumidor e soberania digital.

Essa discussão já não se atém às redes sociais, aos motores de busca ou aos sistemas de publicidade comportamental, alcançando também as atividades inseridas na economia digital descentralizada, a exemplo da mineração de criptomoedas, que embora costume ser descrita apenas sob prisma técnico ou financeiro, depende de fluxos informacionais, dispositivos de autenticação, monitoramento de desempenho, geolocalização, infraestrutura em nuvem, sistemas de pagamento e ambientes digitais controlados ou influenciados por grandes empresas de tecnologia. Nesse prisma, a mineração figura como espaço relevante para examinar como dados, infraestrutura e poder econômico se articulam.

A LGPD (Lei nº 13.709/2018), editada com a promessa de reequilibrar a relação entre titulares e agentes de tratamento, passou a conviver com modelos de negócios dependentes de coleta massiva, perfilização e experimentação algorítmica, muitas vezes conduzidos por corporações transnacionais com recursos jurídicos e tecnológicos muito superiores aos de empresas nacionais e às próprias instituições de controle. Surge, nessa ótica, a dúvida que orienta este artigo: no contexto brasileiro, a LGPD efetivamente limita o poder das *big techs* ou, em determinadas condições, acaba operando como instrumento que legitima e aumenta esse poder sob o rótulo da conformidade regulatória?

A mesma indagação ganhou novas nuances quando observada a partir da mineração de criptomoedas. Isso porque, mesmo em um ambiente associado ao ideal de descentralização, muitos de seus arranjos materiais e informacionais passam por serviços ofertados por grandes plataformas tecnológicas, o que levanta a pergunta sobre se a proteção de dados, nesse campo, funciona como limite jurídico à concentração de poder ou se acaba sendo absorvida por estruturas privadas que aumentam dependências técnicas, econômicas e regulatórias.

Nesse caminho, o objetivo deste artigo é avaliar em que medida a LGPD atua, na prática, como obstáculo ou como ferramenta de materialização do poder das grandes plataformas digitais no Brasil, considerando, em perspectiva aplicada, a forma como essa dinâmica também se apresenta na economia da mineração de criptomoedas. Para tanto, trata-se de pesquisa qualitativa, de natureza jurídico-teórica e documental, ancorada em método predominantemente dedutivo. Parte-se da estrutura normativa da LGPD e de seu enquadramento constitucional para, a partir daí, examinar situações que envolvem *big techs* no contexto brasileiro.

Como recorte complementar, o trabalho também observa situações em que infraestruturas, serviços e ambientes tecnológicos vinculados à mineração de criptomoedas dependem de coleta, circulação ou tratamento de dados pessoais, seja em mecanismos de cadastro, verificação, monitoramento operacional ou intermediação digital.

O percurso metodológico inicia com uma revisão da legislação aplicável, como a Constituição, LGPD, Marco Civil da Internet, Emenda Constitucional n.º 115/2022 e atos normativos da ANPD, bem como de documentos oficiais produzidos por autoridades de proteção de dados, órgãos de defesa da concorrência e entidades de defesa do consumidor. Em seguida, foi feita a análise de decisões selecionadas do STF, do STJ, da ANPD e do CADE, com recorte temporal que se estende da entrada em vigor da LGPD até o ano de 2025, privilegiando controvérsias em que estejam em jogo o tema em questão.

A justificativa da pesquisa se sustenta em dimensões teóricas e práticas. Do ponto de vista teórico, há necessidade de ampliar a compreensão da proteção de dados pessoais como eixo estruturante da ordem econômica digital, indo além da leitura tradicional centrada exclusivamente na tutela da intimidade.

No plano prático, o tema ganha importância diante da crescente dependência de serviços e infraestruturas controlados por grandes plataformas, da atuação ainda recente da ANPD e da multiplicação de controvérsias judiciais envolvendo vazamentos, perfilização, publicidade comportamental e integração de dados entre diferentes serviços de uma mesma corporação.

Bem como, soma-se a isso a expansão de atividades digitais que, embora associadas ao discurso da descentralização, permanecem materialmente vinculadas a grandes infraestruturas privadas, como ocorre em segmentos da mineração de criptomoedas, tornando pertinente analisar se a LGPD pode atuar nesse campo como vetor de contenção de assimetrias ou se acaba coexistindo com novas formas de dependência tecnológica.

2 A LGPD NO CONTEXTO DO DIREITO BRASILEIRO: FUNDAMENTOS, PRINCÍPIOS E DESAFIOS DE IMPLEMENTAÇÃO

A positivação da proteção de dados pessoais no Brasil decorreu de um processo gradual de constitucionalização da privacidade em ambiente digital, em diálogo com a expansão das tecnologias de vigilância, de coleta massiva de informações e com o modelo de negócios baseado em dados que marca a atuação das maiores empresas de tecnologia. Para Zuboff (2019), a apropriação de dados de comportamento transforma a experiência humana em matéria-prima para predição e controle, o que desafia categorias clássicas do direito privado e do direito público.

Em contexto semelhante, Rodotà (2008) mostra como a privacidade é uma expressão das condições mínimas de liberdade em sociedades estruturadas por sistemas de monitoramento contínuo. Quando esse cenário é transplantado para a realidade brasileira, marcada por desigualdades históricas e assimetrias de poder informacional, a proteção de dados integra o núcleo de garantias indispensáveis ao exercício da cidadania e à contenção de abusos econômicos ligados à exploração de dados pessoais (Frazão, 2018a).

A Constituição de 1988 já oferecia uma base importante para esse movimento ao assegurar a inviolabilidade da intimidade, da vida privada, da honra e da imagem (art. 5º, X), o sigilo das comunicações (art. 5º, XII) e o habeas data (art. 5º, LXXII), permitindo a defesa do indivíduo diante de bancos de dados e registros estatais ou privados (Brasil, 1988). A doutrina passou a ler esses dispositivos à luz da categoria da autodeterminação informativa, desenvolvida inicialmente na jurisprudência

alemã, para sustentar que o indivíduo deve poder decidir, em condições minimamente livres, sobre a coleta, o uso e a circulação de suas informações pessoais (Mendes, 2014).

Sarlet (2021) argumenta que, mesmo antes da inclusão expressa da proteção de dados no texto constitucional, já havia um direito à tutela dos dados pessoais deduzido da combinação entre direitos da personalidade, garantias de sigilo e cláusula geral de proteção da dignidade, de modo a exigir do Estado deveres positivos de organização institucional e de controle sobre o tratamento de dados.

Esse entendimento foi acolhido pela jurisprudência do Supremo Tribunal Federal no julgamento da ADI 6.387, em que se discutiu a constitucionalidade da Medida Provisória n. 954/2020, que determinava o compartilhamento de dados de usuários de telefonia com o IBGE. Ao suspender a vigência da medida, o Tribunal reconheceu expressamente a existência de um direito à proteção de dados pessoais, apontando que a simples circulação massiva de cadastros sem salvaguardas adequadas já representa risco à liberdade e à igualdade em ambiente digital (STF, ADI 6.387/DF).

Com a Emenda Constitucional n. 115/2022, esse direito ganhou menção explícita no art. 5º, LXXIX, e a competência para legislar sobre proteção e tratamento de dados foi fixada como privativa da União (arts. 21, XXVI, e 22, XXX), consolidando a proteção de dados pessoais como eixo estruturante da ordem constitucional brasileira em matéria de tecnologia e informação (Brasil, 2022).

A LGPD se inseriu nesse quadro como norma geral que concretiza, em nível infraconstitucional, os valores e deveres ligados ao tratamento de dados pessoais. O art. 1º estabelece que a lei tem por objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018), sinalizando que o tratamento de dados é um problema de tutela da personalidade em contexto de *datafication* intensa (Doneda, 2011).

O art. 2º explicita princípios orientadores como o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, o desenvolvimento econômico e tecnológico e a defesa do consumidor, ampliando a ideia de que a LGPD opera em chave transversal, entre direito constitucional, direito civil, direito do consumidor e regulação econômica (Sarlet; Saavedra, 2020).

Os princípios do art. 6º organizam o modo como o tratamento de dados deve ocorrer no plano cotidiano: finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas (Brasil, 2018).

A incidência desses princípios também irradia efeitos sobre ambientes digitais associados à mineração de criptomoedas, mormente quando essa atividade envolve *pools*, plataformas de gerenciamento remoto, soluções de hospedagem, *marketplaces* de equipamentos, painéis de desempenho, sistemas de autenticação em múltiplos fatores e mecanismos de prevenção à fraude.

Nesses ambientes, informações cadastrais, endereços IP, padrões de uso, dados de localização, métricas de desempenho e registros de acesso podem ser tratados de forma contínua, exigindo leitura da LGPD que ultrapasse o campo mais óbvio da publicidade comportamental e abarque estruturas digitais voltadas à validação distribuída e à exploração econômica de ativos criptográficos.

Tais vetores funcionam como critérios de interpretação e de controle da atividade dos agentes de tratamento, exigindo que o uso de dados seja limitado ao estritamente necessário, que os titulares compreendam como e por que seus dados são utilizados e que existam medidas técnicas e organizacionais capazes de reduzir riscos de incidentes e de discriminação algorítmica.

Tanto Bioni (2019) quanto Frazão (2018b) entendem que essa estrutura aproxima a LGPD de um modelo de regulação baseado em gestão de riscos e em governança de dados, em que o responsável pelo tratamento deve demonstrar, de forma documentada, a conformidade de seus processos com a lei.

As bases legais do art. 7º e os requisitos específicos do art. 11 complementam esse desenho, ao listar hipóteses nas quais o tratamento de dados é juridicamente admitido, como exemplo, consentimento, cumprimento de obrigação legal ou regulatória, execução de contrato, exercício regular de direitos, proteção da vida ou da incolumidade, tutela da saúde, legítimo interesse, entre outras (Brasil, 2018).

A lei afasta a ideia de que o consentimento seria a única via legítima para o tratamento, porém exige que, sempre que ele seja a base escolhida, deva ser livre, informado e inequívoco, com possibilidade real de revogação pelo titular, o que supõe linguagem clara, apresentação destacada e opções de recusa sem retaliação contratual (Bioni, 2019).

Nas bases ligadas a deveres legais, políticas públicas ou legítimo interesse, a ênfase recai sobre o dever de demonstrar a necessidade do tratamento, a proporcionalidade entre fins e meios e o respeito a expectativas razoáveis dos titulares, sob pena de o fundamento jurídico se converter, na prática, em autorização vazia para coleta e uso excessivo de dados (Cavalcanti; Santos, 2019).

No plano subjetivo, a LGPD distingue os papéis de controlador, operador e encarregado. Controlador é a pessoa natural ou jurídica responsável pelas decisões referentes ao tratamento, já o operador é quem realiza o tratamento em nome do controlador e o encarregado (DPO) é o canal de comunicação entre controlador, titulares e Autoridade Nacional, com atribuições ligadas a orientação interna e recebimento de reclamações (art. 5º, VI, VII e VIII; art. 41) (Brasil, 2018).

Tal repartição de funções permite alocar deveres de conformidade de forma diferenciada: ao controlador cabe definir finalidade, base legal, prazo de retenção e medidas de governança; ao operador, garantir que o tratamento ocorra dentro das instruções e com segurança adequada; ao encarregado, fomentar uma cultura interna de proteção de dados, mapear riscos e dialogar com titulares e com a ANPD (Opice Blum; Maldonado, 2021).

Os direitos dos titulares, previstos principalmente no art. 18, completam a estrutura normativa, ao assegurar prerrogativas como confirmação de tratamento, acesso,

correção, anonimização, bloqueio ou eliminação de dados desnecessários, portabilidade, informação sobre compartilhamentos e sobre a possibilidade de não consentir, além da revogação do consentimento e da oposição ao tratamento em hipóteses específicas (Brasil, 2018).

Tal percepção é ainda mais saliente quando se percebe que atividades vinculadas à mineração de criptomoedas, apesar de frequentemente apresentadas como impessoais ou puramente técnicas, podem envolver decisões automatizadas de bloqueio de contas, restrições de acesso, monitoramento de dispositivos e cruzamento de informações para fins de segurança, *compliance* e gestão operacional.

Em situações assim, os direitos de acesso, correção, oposição e informação sobre compartilhamento ganham importância, já que o titular enfrenta ambientes técnicos pouco transparentes, nos quais o controle sobre os próprios dados é reduzido pela assimetria entre usuário e operador da infraestrutura.

Esses direitos concretizam, em chave procedimental, a ideia de autodeterminação informativa, ao criar instrumentos para que a pessoa acompanhe o ciclo de vida de seus dados, questione decisões automatizadas e reaja a assimetrias informacionais que favorecem empresas e plataformas digitais (Ruaro; Rodriguez; Finger, 2011).

Em sociedades marcadas por forte desigualdade socioeconômica, o uso desses direitos tende a ser mais difícil para grupos vulnerabilizados, que enfrentam barreiras educacionais, tecnológicas e territoriais, o que aumenta a necessidade de políticas públicas de educação digital e de atuação proativa da ANPD e de órgãos de defesa do consumidor (Santos, 2022).

A Autoridade Nacional de Proteção de Dados surge, nesse cenário, como órgão central da arquitetura institucional da LGPD. Os arts. 55-A a 55-J da lei descrevem suas competências, como elaborar diretrizes para a Política Nacional de Proteção de Dados, zelar pela observância da legislação, fiscalizar e aplicar sanções, promover estudos sobre práticas de proteção de dados e incentivar padrões técnicos compatíveis com a proteção à privacidade (Brasil, 2018). A ANPD também exerce funções normativas, ao editar regulamentos sobre temas como relatórios de impacto, incidentes de segurança, bases legais e dosimetria de sanções, o que lhe confere papel relevante na concretização da LGPD em setores variados, do poder público às plataformas digitais globais (Cravo, 2021).

Apesar desse desenho, Morozov (2018) tem chamado atenção para os desafios enfrentados pela autoridade brasileira. A assimetria tecnológica e econômica em relação às *big techs*, que operam em escala transnacional, dificulta a fiscalização efetiva de práticas opacas de tratamento de dados, como perfis comportamentais elaborados por algoritmos proprietários e opacos.

Questões como transferência internacional de dados, concentração de poder de mercado em plataformas digitais e dependência de infraestruturas estrangeiras colocam a proteção de dados em diálogo com temas de soberania digital e de regulação da economia de plataformas (Pereira; Faleiros Júnior, 2024).

De modo geral, a LGPD, lida a partir da Constituição de 1988 e da atuação da ANPD, mostra um campo do direito brasileiro em que a proteção de dados pessoais está ligada, ao mesmo tempo, à tutela da personalidade, ao controle do poder econômico e à preservação de espaços mínimos de liberdade em uma sociedade orientada por dados.

A consolidação dessa agenda depende da continuidade do desenvolvimento jurisprudencial iniciado pelo STF, da densificação doutrinária sobre o alcance do direito à proteção de dados e da construção de capacidades institucionais que permitam enfrentar práticas lesivas em ambientes marcados pela presença dominante de empresas transnacionais do setor de tecnologia.

3 BIG TECHS E O EXERCÍCIO DE PODER NO TERRITÓRIO BRASILEIRO: TENSÕES ENTRE DIREITO, MERCADO E SOBERANIA DIGITAL

O avanço das grandes empresas de tecnologia no território brasileiro mudou a forma como se exercem poder econômico, comunicação social e mesmo competências típicas do Estado, em um cenário em que os dados pessoais se tornam insumo para modelos de negócio baseados em vigilância e predição de comportamentos.

Conforme já citado, a Carta Magna, ao consagrar a dignidade da pessoa humana, a privacidade e a proteção da intimidade, já apresentava a base para limitar práticas invasivas, entendimento reforçado quando o Supremo Tribunal Federal reconheceu a proteção de dados como direito fundamental autônomo no julgamento que suspendeu a transferência massiva de dados de telecomunicações ao IBGE (ADIs sobre a MP 954/2020). Tal movimento foi consolidado com a Emenda Constitucional nº 115/2022, que incluiu expressamente a proteção de dados pessoais no rol de direitos fundamentais, exigindo leitura com a ordem econômica e a disciplina da livre concorrência.

Os modelos de exploração econômica de dados pessoais empregados por grandes plataformas no Brasil combinam coleta massiva, cruzamento de bases, publicidade comportamental e construção de perfis automatizados, muitas vezes em contextos de assimetria informacional extrema. A lógica de capitalismo de vigilância descrita por Zuboff (2019) ajuda a entender como o comportamento dos usuários é capturado, analisado e convertido em previsões comercializáveis, em um circuito de extração que tende à opacidade e à concentração.

No ambiente brasileiro, esses modelos impactam direitos de consumidores e usuários, pois os serviços aparentemente gratuitos são financiados pela monetização de informações pessoais, muitas vezes com cláusulas contratuais extensas, linguagem técnica e consentimentos obtidos em ambiente de hipervulnerabilidade (Segundo; Couto, 2022).

A doutrina ensina que, em contextos marcados por desequilíbrios de poder e informação, o consentimento isolado deixa de ser elemento suficiente, razão pela qual se reforça a leitura da LGPD à luz da vulnerabilidade do

titular e da necessidade de controles objetivos sobre a proporcionalidade do tratamento (Bioni, 2020).

Além do consentimento, o regime de bases legais e de deveres de controladores, operadores e encarregados amplia a ideia de que o tratamento de dados é atividade sujeita a deveres de cuidado, transparência e prestação de contas diante da autoridade e dos titulares. O controlador passa a responder pela definição das finalidades e pela escolha de meios adequados, enquanto o operador deve observar estritamente as instruções recebidas, sem se apropriar dos dados para interesses próprios, e o encarregado atua como ponto de contato e mecanismo de governança interna (Mendes *et al*., 2021).

Quando plataformas estruturam suas arquiteturas de interface para induzir escolhas favoráveis à coleta máxima de dados, com opções pouco claras de recusa ou com empurrões para o aceite, existem indícios de violação da LGPD e de normas de proteção do consumidor, dada a hipervulnerabilidade informacional dos usuários.

No plano concorrencial, a exploração intensiva de dados por essas empresas aumenta a concentração de mercado e produz barreiras para pequenas e médias empresas brasileiras. Zanatta e Abramovay (2019) explica como o acúmulo de grandes bases de dados, combinado com efeitos de rede e integração vertical, permite que plataformas controlem o acesso a públicos, ajustem os termos de visibilidade de anunciantes e imponham condições contratuais que esvaziam a liberdade negocial de agentes menores.

Essa lógica de concentração alcança setores ligados à economia dos criptoativos, inclusive a mineração de criptomoedas, em que agentes menores dependem de serviços de nuvem, infraestrutura de processamento, hospedagem de dados, meios de pagamento, sistemas operacionais, canais de distribuição de *software* e serviços de autenticação muitas vezes oferecidos por grandes corporações tecnológicas. Ainda que a validação distribuída seja apresentada como expressão de descentralização, a operação cotidiana da mineração pode permanecer vinculada a camadas concentradas de infraestrutura, criando dependências econômicas e informacionais que aproximam esse ecossistema da lógica de poder já observada nas *big techs*.

Krein (2018), em um estudo sobre o uso de dados pelo Facebook, ressalta que modelos baseados em coleta e cruzamento extensivo de informações pessoais podem gerar novos trustes, em que o poder de mercado decorre menos da infraestrutura física e mais da capacidade de controlar fluxos informacionais e de publicidade segmentada.

Esse quadro coloca em tensão o regime constitucional da livre concorrência e da defesa do consumidor com o poder econômico das plataformas, exigindo atuação da LGPD, direito antitruste e regulação setorial. Sobre tal questão, Portela, Zambão e Séllos-Knoerr (2023) tem chamado atenção para a necessidade de que autoridades como CADE e ANPD interpretem práticas de coleta excessiva, auto-preferência em resultados de busca, discriminação de acesso a APIs e mudanças abruptas em algoritmos de recomendação como possíveis formas de abuso de posição dominante e de fechamento de mercado, com efeitos sobre a pluralidade informacional e a diversidade de fontes.

Quando poucas empresas passam a controlar os canais pelos quais notícias circulam, anúncios são exibidos e aplicações de terceiros alcançam usuários, o risco é econômico e democrático, posto que a circulação de ideias se torna dependente de arquiteturas definidas por interesses privados (Castro, 2025).

A relação do Estado brasileiro com essas empresas, sob tal enfoque, é marcada por conflitos regulatórios em que se confrontam argumentos de liberdade econômica, inovação e competitividade com a exigência de proteção de dados, defesa do consumidor, combate à desinformação e tutela de direitos fundamentais.

Nessa esteira, a noção de soberania digital ganha notoriedade quando se observa que infraestruturas, como serviços de nuvem governamental, comunicações estratégicas e mesmo bases de dados educacionais podem ser operados por empresas estrangeiras cujas decisões de negócio não se submetem, de forma integral, ao controle público nacional (Polido, 2024).

A ideia de colonialismo de dados, trabalhada por Silveira, Cassino e Souza (2021) descreve justamente essa dinâmica em que fluxos massivos de dados brasileiros alimentam modelos de negócio globais, enquanto o país permanece dependente de tecnologias, protocolos e plataformas sobre as quais tem pouca ingerência.

O problema é ainda mais visível quando se observa a mineração de criptomoedas em escala profissional. Embora o protocolo da rede possa ser distribuído, a atividade depende de fornecimento energético, chips especializados, conectividade, hospedagem, monitoramento remoto e integração com serviços digitais muitas vezes sediados fora do país. Quando esse arranjo é atravessado por tratamento de dados pessoais de operadores, usuários, clientes ou participantes de pools, a discussão sobre soberania digital passa a envolver a possibilidade real de subordinação de atividades econômicas locais a estruturas tecnológicas estrangeiras que concentram capacidade material, informacional e contratual.

Outrossim, tal questão envolve capacidade efetiva de definir requisitos de conformidade, impor sanções, exigir transparência algorítmica e garantir que decisões de moderação de conteúdo, remoção de perfis ou alteração de regras de uso levem em conta parâmetros constitucionais brasileiros (Beuron; Cristóvam, 2025).

Nesse âmago, iniciativas normativas que reforçam a LGPD, o Marco Civil da Internet e projetos voltados à regulação de plataformas e inteligência artificial objetivam equilibrar liberdade de iniciativa e inovação com segurança jurídica e tutela de direitos, de forma a impedir que tais empresas atuem como quase soberanos sobre o ambiente informacional brasileiro.

Dessarte, o desafio jurídico está em articular proteção de dados, defesa da concorrência, regulação das comunicações e soberania digital em um desenho institucional capaz de limitar práticas abusivas, reduzir dependências tecnológicas e preservar um espaço público informacional plural, compatível com a Constituição de 1988.

4 A LGPD COMO OBSTÁCULO OU INSTRUMENTO DE PODER DAS BIG TECHS NO BRASIL: UMA REFLEXÃO CRÍTICA

Nessa última parte do trabalho, é apropriado realçar que a concentração de dados produz efeitos concorrenciais relevantes, considerando que a capacidade de combinar informações de diferentes serviços, como e-mail, mensageria, redes sociais, nuvem, sistemas operacionais móveis, multiplica o valor da base de dados para fins de segmentação e experimentação algorítmica, aumentando barreiras à entrada para novos *players* que não dispõem da mesma escala e diversidade de fontes (Frazão, 2020).

Estudos do CADE (2023) sobre mercados digitais mostram que a integração vertical entre coleta de dados, infraestrutura de nuvem e camadas de aplicação aumenta assimetrias de poder econômico, o que exige diálogo entre proteção de dados e direito da concorrência para evitar que a LGPD seja instrumentalizada como mera certificação de boas práticas, sem alterar de fato a dinâmica de concentração.

Esse diagnóstico pode ser transportado para a mineração de criptomoedas, especialmente quando se observa a atuação de *pools*, plataformas de gestão, intermediadores e provedores de infraestrutura digital que concentram dados operacionais e cadastrais de seus usuários. Nessas hipóteses, a conformidade formal com a LGPD pode ser mobilizada como argumento de legitimidade, ao passo que permanecem pouco transparentes os critérios de coleta, retenção, compartilhamento e uso de dados em ambientes marcados por dependência técnica e baixa capacidade de auditoria externa.

Logo, o problema não está somente em saber se há política de privacidade ou base legal indicada, como também em verificar se a proteção de dados altera materialmente as relações de poder ou se apenas qualifica juridicamente estruturas já concentradas.

Se, de um lado, o cumprimento formal da LGPD pode ser absorvido com mais facilidade pelas grandes empresas de tecologia, de outro, a fiscalização de práticas abusivas esbarra na opacidade das arquiteturas técnicas e contratuais dessas empresas. A LGPD consagra, no artigo 20, o direito à revisão de decisões automatizadas, todavia, também preserva o segredo comercial e industrial, remetendo a uma ponderação caso a caso entre transparência algorítmica e proteção de ativos intangíveis das empresas (Dourado; Aith, 2022).

Tal desenho normativo abre espaço para que controladores aleguem sigilo empresarial diante de requisições de informação sobre critérios de perfilização, sistemas de recomendação ou modelos de pontuação, o que reduz a capacidade de órgãos públicos avaliarem possíveis práticas discriminatórias ou lesivas à concorrência.

A tese de Renato Leite Monteiro abaliza que o legislador brasileiro foi mais protetivo em relação ao segredo comercial do que o europeu, em grande medida em razão da intensa atuação do setor empresarial durante o processo legislativo da LGPD, deixando claro que a percepção de que a proteção de dados foi desenhada dentro de limites que preservam zonas de opacidade técnica (Monteiro, 2022).

Em consonância, o consentimento muitas vezes obtido por meio de interfaces persuasivas não é suficiente para neutralizar práticas de manipulação sub-reptícia, baseadas em experimentos contínuos com dados comportamentais e em técnicas de microdirecionamento (Santos, 2022). Ou seja, quando combinado com a dificuldade de acesso a informações compreensíveis sobre o funcionamento dos algoritmos, esse cenário coopera com a assimetria entre o indivíduo e a plataforma, inclusive perante o sistema de Justiça, que depende pericialmente de informações fornecidas pelas próprias empresas.

Todavia, infelizmente, a Autoridade Nacional de Proteção de Dados enfrenta limitações materiais e organizacionais para atuar de modo amplo em um ecossistema no qual poucos grupos econômicos concentram milhões de titulares, diversos serviços e fluxos transnacionais intensos. A doutrina de Wimmer (2021) que estuda o *enforcement* da LGPD explica a necessidade de coordenação interinstitucional com órgãos como CADE, Senacon, Ministério Público e Banco Central, sob pena de decisões fragmentadas sobre incidentes que envolvem tanto violações de privacidade quanto práticas de mercado, desinformação, publicidade enganosa ou riscos à democracia.

A própria diretora da ANPD tem falado em eventos públicos que a LGPD não foi pensada para resolver sozinha problemas de concentração econômica, *fake news* ou desigualdades estruturais na esfera digital, exigindo assim a prudência ao projetar expectativas sobre a capacidade da Autoridade (Wimmer, 2020).

O Ministério Público e o sistema de Justiça também esbarram em dificuldades probatórias quando o objeto da controvérsia envolve decisões automatizadas, perfis de risco ou priorização de conteúdo. Ainda que a LGPD crie deveres de transparência, grande parte das informações está protegida por contratos de confidencialidade e por uma interpretação ampliada de segredo de negócio, o que dificulta auditorias sobre potenciais impactos discriminatórios ou efeitos de bloqueio de mercado.

Em atividades ligadas à mineração de criptomoedas, essa opacidade pode aparecer na forma de bloqueios automatizados, encerramento de contas, limitação de acesso a serviços, exigências documentais pouco claras, monitoramento de tráfego e integração de dados entre diferentes camadas da operação. Ainda que parte dessas medidas seja justificada por segurança, prevenção à fraude ou cumprimento regulatório, a ausência de transparência sobre critérios e fluxos de tratamento enfraquece a posição dos titulares e dificulta o controle jurídico sobre práticas potencialmente abusivas.

Ao mesmo tempo, a jurisprudência do STJ sobre vazamento de dados vem exigindo comprovação concreta de dano em incidentes envolvendo dados não sensíveis, afastando a presunção de dano moral *in re ipsa* em decisões como o AREsp 2.130.619/SP, o que reduz o espaço para reparação em larga escala em incidentes que atingem milhões de pessoas, não obstante, têm efeitos individualmente difíceis de quantificar (STJ, 2023).

Nos últimos anos, a atuação administrativa em face de grandes plataformas passou a oferecer exemplos de como a LGPD pode ser manejada para conter abusos e para consolidar padrões de governança digitais em torno dessas empresas.

A exigência de ajustes nos mecanismos de verificação de idade e na oferta de um feed sem necessidade de cadastro demonstra que a autoridade está disposta a enfrentar práticas de coleta excessiva em plataformas com grande capilaridade entre públicos vulneráveis, embora a efetividade dessas medidas dependa de monitoramento e cooperação com outras instâncias regulatórias.

Outro ponto a ser considerado ém suspensão cautelar do tratamento de dados pessoais para treinamento de sistemas de inteligência artificial generativa com base em indícios de falta de transparência e riscos elevados aos titulares brasileiros (ANPD, 2024), podendo haver estabelecimento de multa diária em caso de descumprimento, sendo tal assunto amplamente debatida por organizações da sociedade civil, que apontaram o precedente como exemplo de uso da LGPD para disciplinar novas tecnologias antes da aprovação de uma lei específica de inteligência artificial (Dataprivacy, 2024).

Posteriormente, a Autoridade passou a admitir, com restrições, o retorno do tratamento de dados para fins de IA, mantendo, nada obstante, vedação quanto a certas categorias sensíveis e determinando salvaguardas para menores de idade, o que mostra um diagnóstico de que, em contexto de assimetria informacional tão pronunciada, medidas preventivas podem ser necessárias para reequilibrar a relação entre titulares e plataforma (ANPD, 2024).

Em 2025, a conclusão da análise sobre o compartilhamento de dados pessoais entre duas grandes empresas de uso de dados, no contexto da política de privacidade de 2021, inaugurou um novo patamar de intervenção, tendo em vista que a ANPD reconheceu que o fluxo de dados entre as empresas se dava em dois eixos, sendo um em que a uma delas atuava como operadora, para viabilizar o serviço de mensageria, e outro em que atuava como controladora, principalmente na conexão com outros serviços do grupo, e determinou a contratação de auditoria externa independente, aumento da transparência e ajustes nas bases legais utilizadas para certos tratamentos (ANPD, 2025).

Essa decisão foi saudada por entidades como um passo importante para reequilibrar as condições de uso da infraestrutura de comunicação controlada pela *big tech*, ao mesmo tempo em que majora a percepção de que o próprio reconhecimento da operadora ou controladora em diferentes situações passa por interpretação jurídica controversa, na qual a empresa tende a defender a leitura menos restritiva às suas práticas de integração de dados.

Na esfera concorrencial, o recente Termo de Compromisso de Cessação firmado entre o uma das maiores operadoras de dados mundial e o CADE, em 2025, em investigação sobre possíveis abusos de posição dominante relacionados ao sistema operacional Android e à pré-instalação de aplicativos de busca e navegação, explicita que o poder informacional das plataformas passou a ser objeto de condicionantes específicos em acordos antitruste, ainda que a discussão não se limite à LGPD (CADE, 2025).

Ao admitir que práticas de *tying* e incentivos econômicos podem restringir a capacidade de concorrentes acessarem usuários em condições equânimes, o Conselho dialoga com autores que associam dados pessoais, algoritmos de recomendação e mercados de atenção, sugerindo que a proteção de dados precisa ser articulada a remédios estruturais em direito da concorrência para evitar que a conformidade formal da LGPD conviva com estratégias de exclusão de rivais (Koury; Oliveira, 2022).

No Judiciário, além das decisões sobre vazamentos de dados, começam a surgir controvérsias em que a LGPD é invocada em litígios envolvendo bloqueio de contas, remoção de conteúdo, uso de *cookies* de rastreamento e práticas de publicidade direcionada em plataformas sociais. Em levantamentos da Legalcomply (2024), percebe-se que a lei já é mencionada em milhares de decisões, embora nem sempre como fundamento determinante do resultado, e que ainda há oscilação entre interpretações mais protetivas da autodeterminação informativa e leituras que priorizam a liberdade de iniciativa e a limitação da responsabilidade civil dos controladores.

Nesse caminho, observa-se que o modo como o sistema de Justiça assimila e aplica os comandos da LGPD aos litígios envolvendo *big techs* será pertinente para definir se a lei funcionará como obstáculo real ao exercício abusivo do poder de mercado e do poder informacional ou se acabará operando como uma linguagem jurídica que legitima, sob o rótulo de conformidade, estruturas de dominação algorítmica descritas por autoras como Shoshana Zuboff e Cathy O'Neil.

Sob esse ângulo, a mineração de criptomoedas é um campo promissor para perceber a ambiguidade da LGPD. Por um espectro, a lei pode servir de fundamento para exigir limitação de coleta, transparência, segurança e responsabilização em ecossistemas que atuam sob forte assimetria técnica. Por outra visão, se aplicada apenas em perspectiva formal, pode ser absorvida como elemento de reputação regulatória por agentes que continuam concentrando infraestrutura, dados e poder de definir unilateralmente as condições de acesso ao ambiente digital. Assim sendo, a tensão identificada ao longo deste artigo também aparece em setores que se anunciam como descentralizados, mas que, na prática, convivem com novas formas de intermediação e dependência.

5 CONSIDERAÇÕES FINAIS

A trajetória percorrida ao longo deste artigo deixou claro que a LGPD está em uma encruzilhada, onde pode funcionar como freio ao abuso de dados pelas grandes empresas de tecnologia ou ser reduzida a verniz jurídico para estratégias cada vez mais sofisticadas de dominação algorítmica.

Enquanto as plataformas acumulam dados, cruzam bases, integram serviços e desenham interfaces para extrair o máximo possível de informações, o discurso da conformidade tende a ser incorporado como mais um

ativo competitivo, corroborando com a ideia de que quem tem mais estrutura jurídica e técnica transforma a proteção de dados em vantagem de mercado.

Essa constatação é notória quando se observa a mineração de criptomoedas, frequentemente apresentada como espaço de descentralização e autonomia tecnológica. O trabalho desenvolvido mostrou que, mesmo nesse ambiente, existem dependências relevantes em relação a infraestruturas, serviços e mecanismos de tratamento de dados controlados por grandes agentes econômicos.

Por essa razão, a discussão sobre proteção de dados não pode ficar restrita às redes sociais ou à publicidade comportamental, devendo alcançar também os ecossistemas digitais em que a descentralização do protocolo convive com a concentração material da infraestrutura.

A lei promete reequilibrar forças, não obstante, atua em um ambiente de opacidade técnica, assimetria informacional extrema e concentração econômica, em que decisões automatizadas, sistemas de recomendação e fluxos transnacionais de dados escapam com facilidade ao controle cotidiano de instituições enfraquecidas e de titulares sobrecarregados por consentimentos e políticas de privacidade incompreensíveis.

Ao mesmo tempo, as poucas intervenções mais firmes sobre grandes plataformas mostram que a LGPD tem munição para incomodar quando é aplicada com coragem institucional, ou seja, pode bloquear fluxos de dados, impor mudanças em políticas de privacidade, exigir auditorias externas, condicionar modelos de negócio e conectar proteção de dados com concorrência, defesa do consumidor e soberania digital.

Logo, finalizamos este artigo afirmando que o ponto mais importante não está no texto da lei, mas sim em como o sistema de justiça, as autoridades regulatórias e a própria sociedade vão escolher utilizá-la.

Ou a LGPD é manejada como instrumento de enfrentamento real ao colonialismo de dados e à captura do ambiente informacional brasileiro por poucos conglomerados, inclusive nos setores emergentes da economia digital, como a mineração de criptomoedas, ou será incorporada, sem maior resistência, ao vocabulário de *marketing* regulatório das grandes empresas, funcionando como selo de respeitabilidade para modelos de exploração que seguem reproduzindo assimetrias técnicas, econômicas e informacionais.

O futuro da proteção de dados no Brasil passa, em larga medida, pela capacidade de perceber que o poder das *big techs* se exerce onde os dados circulam de forma visível e nos bastidores infraestruturais que sustentam novas atividades digitais.

REFERÊNCIAS

ANPD. Autoridade Nacional de Proteção de Dados. **ANPD abre processo sancionador e emite determinações ao TikTok.** Brasília, DF, 4 nov. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-processo-sancionador-e-emite-determinacoes-ao-tiktok. Acesso em: 19 mar. 2026.

ANPD. Autoridade Nacional de Proteção de Dados. **ANPD conclui a análise sobre compartilhamento de dados pessoais entre WhatsApp e Meta.** Brasília, DF, 11 nov. 2025. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-conclui-a-analise-sobre-compartilhamento-de-dados-pessoais-entre-whatsapp-e-meta. Acesso em: 19 mar. 2026.

ANPD. Autoridade Nacional de Proteção de Dados. **ANPD determina suspensão cautelar do tratamento de dados pessoais para treinamento da IA da Meta.** Brasília, DF, 2 jul. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta. Acesso em: 19 mar. 2026.

BEURON, Bruno Mello Corrêa de Barros; CRISTÓVAM, José Sérgio da Silva. Colonialismo de dados, obscurantismo tecnológico e opacidade informacional: os novos riscos e desafios de proteção dos direitos fundamentais e da soberania digital no ângulo da governança pública digital. **Revista Democracia Digital e Governo Eletrônico**, Florianópolis, v. 1, n. 24 esp., p. 107-125, 2025.

BIONI, Bruno Ricardo et al. A landmark ruling from the Brazilian Supreme Court: data protection as an autonomous fundamental right and informational due process. **European Data Protection Law Review**, v. 6, n. 4, p. 615-624, 2020.

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

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: a função e os limites do consentimento. Rio de Janeiro: Forense, 2020.

BRASIL. **Emenda Constitucional nº 115, de 10 de fevereiro de 2022.** Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União, Brasília, DF, 11 fev. 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc115.htm. Acesso em: 19 mar. 2026.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da União, Brasília, DF, 5 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 19 mar. 2026.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 19 mar. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário

Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 mar. 2026.

BRASIL. Superior Tribunal de Justiça. **Agravo em Recurso Especial nº 2.130.619/SP.** Rel. Min. Francisco Falcão. Segunda Turma, julgado em 7 mar. 2023, DJe 10 mar. 2023. Disponível em: https://buscadordizerodireito.com.br/jurisprudencia/11482/o-vazamento-de-dados-pessoais-nao-gera-dano-moral-presumido. Acesso em: 19 mar. 2026.

CADE. Conselho Administrativo de Defesa Econômica. **Cadernos do CADE – Plataformas digitais.** Brasília, DF: CADE, 2021. Disponível em: https://cdn.cade.gov.br/Portal/centrais-de-conteudo/publicacoes/estudos-economicos/cadernos-do-cade/plataformas-digitais.pdf. Acesso em: 19 mar. 2026.

CADE. Conselho Administrativo de Defesa Econômica. **Termo de Compromisso de Cessação – Google/Android (aprovado em 10 dez. 2025).** Brasília, DF: CADE, 2025.

CASTRO, Leonardo Bellini de. Direitos fundamentais e relações privadas na era das big techs: o novo desafio do século XXI. **Revista de Direito Constitucional e Internacional**, São Paulo, v. 152, n. 2, nov./dez. 2025.

COUTO, José Henrique Oliveira. Vazamentos de dados e dano moral'in re ipsa': comentários ao Agravo em Recurso Especial nº 2.130. 619/SP. **Revista IBERC**, v. 6, n. 2, p. 171-188, 2023.

CRAVO, Daniel Corrêa (org.). **Lei Geral de Proteção de Dados e o poder público**. Porto Alegre: Procempa, 2021.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2020.

DOURADO, Daniel de Araujo; AITH, Fernando Mussa Abujamra. The regulation of artificial intelligence for health in Brazil begins with the General Personal Data Protection Law. **Revista de Saúde Pública**, v. 56, p. 80, 2022.

FRAZÃO, Ana. Data-driven economy e seus impactos sobre os direitos de personalidade: indo além da privacidade e do controle aos dados pessoais. **Jota**, São Paulo, 18 jul. 2018a.

FRAZÃO, Ana. Nova LGPD: principais repercussões para a atividade empresarial. **Jota**, São Paulo, 29 ago. 2018b.

FRAZÃO, Ana. Objetivos e alcance da LGPD. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (org.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

FRAZÃO, Ana. **Plataformas digitais e o negócio de dados**. In: FERRAZ JR., Tércio Sampaio (coord.). Direito concorrencial e plataformas digitais. São Paulo: Thomson Reuters Brasil, 2020.

KOURY, Suzy Elizabeth; OLIVEIRA, Lis Arrais. A política nacional de proteção de dados pessoais e da privacidade: a defesa do consumidor e da livre concorrência. **Revista Húmus**, São Luís, v. 12, n. 36, 2022.

KREIN, Julia. Novos trustes na era digital: efeitos anticompetitivos do uso de dados pessoais pelo Facebook. **Revista de Defesa da Concorrência**, Brasília, v. 6, n. 1, 2018.

MENDES, Laura Schertel et al. (coord.). **Tratado de proteção de dados pessoais**. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel Ferreira. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MENDES, Laura Schertel. **A Lei Geral de Proteção de Dados Pessoais**: um modelo de aplicação em três níveis. In: MENDES, Laura Schertel et al. (org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor**: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MONTEIRO, Renato Leite. **Desafios para a efetivação do direito fundamental à proteção de dados pessoais**. 2022. Tese (Doutorado em Direito) – Universidade de São Paulo, São Paulo, 2022.

MOROZOV, Evgeny. **Big tech**. Ubu Editora LTDA-ME, 2018.

O'NEIL, Cathy. **Weapons of math destruction**: how big data increases inequality and threatens democracy. New York: Crown, 2016.

PEREIRA, Laurence Duarte Araújo; JÚNIOR, José Luiz de Moura Faleiros. Regulação das plataformas digitais no Brasil e a defesa da soberania nacional. **Revista de Ciências do Estado**, v. 9, n. 1, p. 1-22, 2024.

POLIDO, Fabrício Bertini Pasquot. Estado, soberania digital e tecnologias emergentes: interações entre direito internacional, segurança cibernética e inteligência artificial. **Revista de Ciências do Estado**, Belo Horizonte, v. 9, n. 1, p. 1-30, 2024.

PORTELA, Irene; ZAMBÃO, Lara Helena Luiza; SÉLLOS-KNOERR, Viviane Coêlho. A coleta de dados pessoais e a violação aos direitos humanos: diálogo das

possíveis consequências para os direitos humanos e o ecossistema empresarial. **Revista Em Tempo**, v. 22, n. 1, p. 283-296, 2023.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

SANTOS, Iara de Araújo. A vulnerabilidade dos titulares de dados diante de grandes plataformas e big techs: um paralelo entre as violações ao GDPR e à LGPD no que tange à base legal do consentimento. Revista de Direito, Estado e Telecomunicações, Brasília, v. 14, n. 2, 2022.

SARLET, Ingo Wolfgang. O direito fundamental à proteção de dados pessoais na Constituição Federal brasileira de 1988. **Revista Privacidade e Proteção de Dados**, v. 1, n. 1, p. 12-49, 2021.

SEGUNDO, Elpídio Paiva Luz; COUTO, Eliane Lopes. A proteção de dados e a hipervulnerabilidade do consumidor sob a perspectiva do consentimento e privacidade na internet. **Revista Jurídica Cesumar**, Maringá, v. 22, n. 3, p. 551-566, 2022.

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

WIMMER, Miriam. **Os desafios do enforcement na LGPD**: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. In: MENDES, Laura Schertel et al. (org.). Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

ZANATTA, Rafael Augusto Ferreira; ABRAMOVAY, Ricardo. Dados, vícios e concorrência: repensando o jogo das economias digitais. **Estudos Avançados**, São Paulo, v. 33, n. 96, p. 421-446, 2019.

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