Jornal of Legal Sciences
Pensar
e-ISSN: 2317-2150
Universidade de Fortaleza

10.5020/2317-2150.2025.15201

O direito à proteção de dados pessoais na fronteira do capitalismo de dados e do colonialismo digital[1]

The right to personal data protection on the frontier of data capitalism and digital colonialism

El derecho a la protección de datos personales en la frontera del capitalismo de datos y del colonialismo digital

João Pedro Seefeldt Pessoa *[2], *Universidad de León, León, Espanha

Têmis Limberger[**3], **Pedro Victor dos Santos Witschoreck**[**4], Universidade do Vale do Rio dos Sinos, Porto Alegre, Rio Grande do Sul, Brasil

Editorial

Histórico do Artigo
Recebido: 24/04/2024
Aceito: 20/12/2024

Eixo Temático 3: Direito, Tecnologia e Sociedade em Transformação

Editores-chefes
Katherinne de Macêdo Maciel Mihaliuc
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
katherinne@unifor.br

Sidney Soares Filho
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
sidney@unifor.br

Editor Responsável
Sidney Soares Filho
Universidade de Fortaleza, Fortaleza, Ceará, Brasil
sidney@unifor.br

Autores
João Pedro Seefeldt Pessoa
jpseefeldt@gmail.com
Contribuição: Conceptualization, Methodology, Investigation, Writing - Original Draft.

Têmis Limberger
temisl@unisinos.br
Contribuição: Supervision.

Pedro Victor dos Santos Witschoreck
pedroviktor@hotmail.com
Contribuição: Writing – Review & Editing.

Como citar:
PESSOA, João Pedro Seefeldt; Limberger, Têmis; Witschoreck, Pedro Victor dos Santos. O direito à proteção de dados pessoais na fronteira do capitalismo de dados e do colonialismo digital. Pensar – **Revista de Ciências Jurídicas**, Fortaleza, v. 30, e15201, 2025. DOI: https://doi.org/10.5020/2317-2150.2025.15201

Declaração de disponibilidade de dados

A Pensar – Revista de Ciências Jurídicas adota práticas de Ciência Aberta e disponibiliza, junto à presente publicação, a Declaração de Disponibilidade de Dados (Formulário Pensar Data) preenchida e assinada pelos autores, a qual contém informações sobre a natureza do artigo e a eventual existência de dados complementares. O documento pode ser consultado como arquivo suplementar neste site.

Resumo

O presente artigo pretende observar o desenvolvimento de modelos regulatórios do direito à proteção de dados pessoais, analisando como o modelo atual de regulação, fundado na livre circulação de dados, legitima o capitalismo de dados e fortalece o colonialismo digital do Sul Global, com ênfase na Lei Geral de Proteção de Dados Pessoais. Para tanto, adota-se o método de abordagem fenomenológico-hermenêutico, o método de procedimento monográfico e comparativo, bem como técnicas de pesquisa de documentação indireta e revisão de bibliografia. Conclui-se que a legislação brasileira de proteção de dados, ao se inspirar na regulamentação europeia, pode, inadvertidamente, refletir padrões de capitalismo de dados e de colonialismo digital, considerando que o controle dos dados pessoais pelos titulares é inexistente em meio à economia digital dominada pelas grandes corporações tecnológicas.

Palavras-chave: Big techs; capitalismo de dados; colonialismo digital; direto à proteção de dados pessoais.

Abstract

This article aims to observe the development of regulatory models for the right to personal data protection, analyzing how the current regulatory model, based on the free circulation of data, legitimizes data capitalism and strengthens the digital colonialism of the Global South, with an emphasis on the General Law for the Protection of Personal Data. To this end, a phenomenological-hermeneutic approach, a monographic and comparative procedure method, indirect documentation research techniques, and a literature review were adopted. It is concluded that the Brazilian Data Protection Legislation, inspired by European regulations, may inadvertently reflect patterns of data capitalism and digital colonialism, considering that control over personal data by data subjects is non-existent amid the digital economy dominated by large technology corporations.

Keywords: *Big tech; data capitalism; digital colonialism; right to personal data protection.*

Resumen

El presente artículo pretende observar el desarrollo de modelos regulatorios del derecho a la protección de datos personales, analizando cómo el modelo actual de regulación, fundado en la libre circulación de datos, legitima el capitalismo de datos y fortalece el colonialismo digital del Sur Global, con énfasis en la Ley General de Protección de Datos Personales. Para tanto, se adopta el método de enfoque fenomenológico-hermeneútico, el método de procedimiento monográfico y comparativo, como también técnicas de investigación de documentación indirecta y revisión de bibliografía. Se concluye que la legislación brasileña de protección de datos, al inspirarse en la reglamentación europea, puede, inadvertidamente, reflejar modelos de capitalismo de datos y de colonialismo digital, considerando que el control de los datos personales por los titulares es inexistente en medio a la economía digital dominada por las grandes corporaciones tecnológicas.

Palabras clave: *Big techs; capitalismo de datos; colonialismo digital; derecho a la protección de datos personales.*

[1] O presente artigo científico foi subvencionado pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Código de Financiamento 001.

[2] Doutor em Direito pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS. Bolsista CAPES/PROEX Mestre em Direito pela Universidade Federal de Santa Maria – UFSM. Mestre em Direito pela Universidad de León – UNILEON (Espanha).

[3] Pós-Doutorado em Direito pela Universidade de Sevilha (Espanha). Doutorado em Direito pela Universidade Pompeu Fabra (Espanha). Mestrado e graduação em Direito pela Universidade Federal do Rio Grande do Sul. Professora do Programa de Pós-Graduação em Direito e Curso de Direito da Universidade do Vale do Rio dos Sinos – UNISINOS.

[4] Doutorando em Direito pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos – UNISINOS. Bolsista CAPES/PROEX. Mestre em Direito pela Universidade Federal de Santa Maria – UFSM.

1 Introdução

A ascensão do capitalismo de dados e a consequente emergência de um novo paradigma de regulação de informações pessoais suscitam um debate crítico e necessário sobre a eficácia das legislações atuais em meio à transformação digital global. No cerne desse debate está a questão de como a regulação sobre o direito à proteção de dados pessoais, notadamente inspirada pelo Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia, reflete o dinamismo do capitalismo de dados e, possivelmente, perpetua uma forma de colonialismo digital.

Considerando a dimensão social e democrática na regulação da proteção de dados, discute-se um contraponto ao capitalismo de dados que, frequentemente, prioriza o lucro em detrimento da privacidade e da autodeterminação informativa. Nesse sentido, o presente artigo questiona em que medida a adoção de regulações do direito à proteção de dados pessoais, especialmente inspiradas em modelos europeus de livre circulação de ativos digitais, pode expressar formas de capitalismo de dados e de colonialismo digital?

O objetivo geral do presente trabalho é, então, problematizar a regulação do direito à proteção de dados pessoais, inspirada em modelos europeus como novas expressões do capitalismo de dados e de colonialismo digital. Em termos específicos, pretende-se: a) abordar o surgimento do capitalismo de dados e o protagonismo das *big techs,* observando o desenvolvimento de modelos regulatórios do direito à proteção de dados pessoais, com especial ênfase no Regulamento Geral de Proteção de Dados Pessoais da União Europeia; e b) compreender como o modelo atual de regulação do direito à proteção de dados pessoais fundado na livre circulação de dados fortalece e legitima o capitalismo de dados, bem como apontar a existência do colonialismo digital do Sul Global, analisando especialmente o caso da Lei Geral de Proteção de Dados Pessoais do Brasil.

Em relação à metodologia de abordagem, adota-se o método fenomenológico-hermenêutico, em razão da necessidade de compreender e interpretar o fenômeno do capitalismo de dados e a regulação do direito à proteção de dados pessoais dentro do quadro social, econômico e jurídico contemporâneo, considerando a interação que o pesquisador possui com o fenômeno do colonialismo digital. Quanto à metodologia de procedimento, elege-se a técnica monográfica e comparativa, que permite aprofundar a análise do tema do capitalismo de dados e do colonialismo digital sob enfoques específicos, especialmente em razão da comparação de modelos regulatórios. Para a coleta de dados, recorre-se à documentação indireta, incluindo a revisão de literatura e a interpretação de dados pertinentes à área de estudo.

2 Sobre o capitalismo de dados e o direito à proteção de dados pessoais

A economia contemporânea testemunha a ascensão dos dados como peça fundamental nas dinâmicas de mercado. Esta nova realidade configura-se pelo capitalismo de dados, em que os dados não são apenas mecanismos de personalização de informações, mas, sim, ativos econômicos cruciais. A coleta e análise de grandes volumes de dados pessoais transformaram-se no motor de um sistema econômico que tem na previsão, modificação e vigilância do comportamento humano fontes de valor monetário sem precedentes (Mayer-Scönberger, 1997; Pessoa, 2020; Zuboff, 2019).

A noção dataísta propõe o universo como um “fluxo de dados e o valor de qualquer fenômeno ou entidade é determinado por sua contribuição ao processamento de dados”, incluindo as relações humanas (Harari, 2015, p. 321). Na sociedade contemporânea, a humanidade está cada vez mais integrada ao processamento de dados, que se tornaram a principal fonte de compreensão e intervenção sobre os indivíduos. Nesse novo paradigma, os dados não são apenas uma ferramenta de observação, sendo também uma maneira de configurar a própria humanidade criando uma relação simbiótica entre as pessoas e os sistemas que processam essas informações (Hui, 2020, p. 77-78).

Nesse contexto, os dados emergem como *commodities* econômicas, cujo valor é ativamente construído por meio de algoritmos, de inteligência artificial e de máquinas. Este processo é intrínseco à lógica de acumulação de capital das *big techs*, grandes corporações empresariais de tecnologia, representadas pelas plataformas digitais (Srnicek, 2016, p. 30-31), que, não apenas coletam dados, mas também tratam e analisam as informações para predizer comportamentos, criando um ciclo contínuo de valorização de suas operações e serviços. A essência desse paradigma reside na capacidade de captar, analisar e utilizar informações como meio para prever e influenciar

comportamentos, criando uma realidade onde o valor gerado transcende à esfera material e adentra as nuances do espaço digital (Pessoa, 2020, p. 40-55).

A transição dos dados – de meros registros digitais para ativos estratégicos – tem sido catalisada pelos modelos de negócios inovadores das *big techs.* Esses modelos de negócios, que se baseiam na monetização da atenção e na manipulação sutil do comportamento dos usuários, são agora paradigmas em várias esferas econômicas. A Google, para muitos, é o maior exemplo dessa revolução social, porque afeta a "nós", "o mundo" e o "conhecimento", numa "googlelização de tudo", justamente "ao catalogar nossos juízos individuais e coletivos, nossas opiniões e (ainda mais importante) nossos desejos, a empresa também vai se transformando numa das mais importantes instituições globais" (Vaidhyanathan, 2011, p. 14).

Trata-se do capitalismo de vigilância, destacado pelo "*superávit comportamental* descoberto mais ou menos já pronto no ambiente on-line, quando se percebeu que a *data exhaust* que entupia os servidores do Google podia ser combinada com as suas poderosas capacidades analíticas para gerar predições de comportamento do usuário" (Zuboff, 2019, p. 404). Dessa maneira, a Google, copiada por outras companhias, "impôs a lógica da conquista, definindo a experiência humana como livre para ser apossada, disponível para ser compilada na forma de dados e reivindicada como ativos de vigilância" (Zuboff, 2019, p. 404).

Os executivos da Google optaram, eventualmente, pelo modelo de negócios baseado em publicidade, que se sustenta na coleta de dados dos usuários para desenvolver e fomentar algoritmos que veiculam anúncios através de um sistema de leilão inovador. A lucratividade excepcional dessa abordagem incentivou outras companhias tecnológicas a adotarem estratégias semelhantes, ampliando a capitalização das gigantes de tecnologia e o escopo da coleta de informações. Tais dados transcendem a mera consequência da utilização de tecnologia pelos usuários; eles são o alicerce de estratégias empresariais que buscam aprimorar a publicidade e customizar os serviços oferecidos, num verdadeiro Grande Outro Irmão (Zuboff, 2018, p. 57-60).

A coleta de dados em larga escala, muitas vezes realizada de maneira não transparente, nutre algoritmos e sistemas de inteligência artificial que fomentam ciclos contínuos de consumo, vigilância e domínio. O mercado é focado em predições e previsões, em que os usuários são o alvo de um comércio não só voltado a atender, mas também a formar e antever suas necessidades. O panóptico, inicialmente projetado como uma estrutura arquitetônica de controle, agora se transforma em um superpanóptico digital ou ciberpanóptico, onipresente, distribuído, fluido e integrado nas tecnologias diárias, de modo que o panoptismo "está vivo e bem de saúde, na verdade, armado de músculos (eletronicamente reforçados, ciborguizados) tão poderosos que Bentham, ou mesmo Foucault, não conseguiria nem tentaria imaginá-lo" (Bauman, 2013, p. 22).

O resultado é uma disparidade de poder, onde alguns se apropriam de vastas quantidades de informação, enquanto a grande maioria permanece à disposição de escolhas feitas por algoritmos, muitas vezes sem seu consentimento ou conhecimento. Dentro deste panorama, os usuários têm pouco ou nenhum conhecimento sobre essa nova dinâmica de informação, uma vez que as vantagens da gratuidade, personalização e rapidez das tecnologias ofuscam os potenciais riscos, ou seja, "raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados" (Rodotà, 2008, p. 37).

No atual contexto socioeconômico, a utilização de dados como ativo econômico e o fenômeno da "digitalização da vida" estão se tornando instrumentos de domínio e reprodução social, com efeitos que se estendem além dos indivíduos, influenciando a sociedade como um todo (Wolfgang, 2021, p. 115). Atualmente, os dispositivos de tratamento de dados influenciam decisões e o próprio corpo social, em um contexto impregnado pela infocracia, traduzido num ambiente onde a geração e manipulação de informações são cruciais para a administração e a dinâmica de poder (Han, 2022).

A monetização dos dados se materializa, principalmente, através da publicidade direcionada e segmentada, que utiliza e vende perfis detalhados dos usuários para anunciantes poderem apresentar anúncios personalizados, o que não apenas fomenta um consumo mais eficiente, mas também perpetua um ciclo de dependência dos dados, onde a privacidade é frequentemente sacrificada em prol de um acesso "gratuito" a plataformas e serviços. Este valor, contudo, não é distribuído de maneira equitativa, mas acumulado nas mãos de poucas corporações que detêm o poder de moldar mercados e influenciar comportamentos sociais (Morozov, 2018, p. 146-147).

A crítica a esses modelos de negócio não se limita à esfera econômica, mas estende-se à dimensão ética e política, uma vez que a acumulação de dados pelas *big techs* suscita questões sobre a soberania dos dados, a

manipulação da opinião pública e o enfraquecimento das instituições democráticas. A influência dessas corporações no espaço público, muitas vezes sem a devida transparência ou responsabilização, representa um desafio para a manutenção de sociedades livres e justas (Morozov, 2018).

A dominância das *big techs* no mercado de tecnologia é inegável, já que grandes corporações, como Google, Amazon, Facebook e Apple – aqui mencionadas pelo nome mais comumente associado, embora façam parte de conglomerados tecnológicos com outras razões empresariais –, não apenas detêm a maior parte do mercado global de tecnologia, mas também desempenham um papel importante na definição de padrões econômicos e sociais. Assim, o poder exercido por essas empresas é sutil e profundamente enraizado nos comportamentos cotidianos, o que as torna ainda mais influente, sendo que, através de algoritmos e plataformas, moldam desde o consumo até a percepção da realidade, criando uma nova forma de poder – psicopoder – difícil de ser contestada ou regulada (Han, 2022, p. 02).

Dessa forma, a solução tecnológica, longe de ser uma panaceia, muitas vezes serve para consolidar o poder nas mãos de poucos, exacerbando a desigualdade e a dependência tecnológica. As *big techs*, com seu poderio econômico e tecnológico, estabelecem as regras do mercado de dados, influenciando políticas públicas e práticas empresariais, muitas vezes em detrimento dos direitos e garantias fundamentais individuais e coletivas (Zuboff, 2019, p. 14-15). Nesse contexto, o exame dos modelos de negócios das *big techs* e a análise de sua dominância e influência é uma progressão que revela a extensão da capacidade dessas entidades de moldar não apenas mercados, mas também sociedades.

A influência se estende ao campo legislativo, onde o *lobby* intensivo dessas corporações pode distorcer a criação de políticas públicas e regulações, favorecendo interesses privados em detrimento do bem comum. A capacidade destas corporações de operarem em múltiplas jurisdições, muitas vezes utilizando-se de estratégias para minimizar obrigações fiscais e regulatórias, coloca-as em uma posição de vantagem em relação aos Estados. A concentração de poder nas mãos de poucas empresas resulta em um ecossistema digital oligopolizado, onde a inovação e a pluralidade podem ser asfixiadas por práticas anticompetitivas.

Além disso, a influência das *big techs* no âmbito da informação é preocupante, uma vez que o controle sobre plataformas de mídias sociais – comumente conhecidas como redes sociais –, mecanismos de busca e outros aplicativos e ferramentas on-line coloca essas corporações em uma posição privilegiada para moldar o discurso público e a formação da opinião (Han, 2018, p. 23-24). Isso desencadeia questões críticas sobre a manipulação de eleições, a disseminação de desinformação e a erosão da confiança nas instituições democráticas, em possíveis algoritmos de destruição em massa (O'Neil, 2020).

Partindo da premissa de que a diversidade de abordagens regulatórias é um reflexo da dinâmica global, é essencial observar a evolução dos marcos regulatórios como um processo contínuo de adaptação e conhecimento da complexidade social. A privacidade e a proteção de dados pessoais estão em constante metamorfose, moldando-se às contínuas inovações tecnológicas e às mudanças nas percepções sociais sobre vida privada e segurança digital (Pérez-Luño, 2012, p. 93), cuja evolução é crucial para manter a relevância dos marcos regulatórios em um mundo onde os dados se tornaram uma mercadoria extremamente valiosa, especialmente diante do contexto da inteligência artificial (Hoch; Engelmann, 2023, p. 11-12).

O desenvolvimento de regulamentações sobre proteção de dados frequentemente segue um padrão reativo, no qual novas leis e diretrizes são introduzidas em resposta a incidentes de violações de dados, avanços tecnológicos disruptivos ou mudanças no comportamento do consumidor (Pessoa, 2020, p. 83-85). Este ciclo de resposta, embora necessário, desafia os legisladores a manterem um equilíbrio entre a proteção dos usuários e a promoção da inovação, posto que as regulamentações devem ser robustas o suficiente para garantir a segurança dos dados pessoais e flexíveis, suficientemente, para se adaptarem a cenários futuros ainda não contemplados, especialmente considerando a complexidade social mediada pelas tecnologias de informação e comunicação.

Diante da importância da privacidade, emerge a necessidade de reconhecer os algoritmos como agentes de interpretação social e entender os metadados como garantias da liberdade tanto individual quanto coletiva. Estas reflexões sublinham a urgência por políticas que estejam em consonância com princípios democráticos no contexto da sociedade digital. Assim, a privacidade, e em particular o direito à proteção de dados pessoais, em um cenário de vigilância tecnológica, ganha relevância na defesa da personalidade humana e na proteção coletiva (Limberger, 2009, p. 46-47).

Observa-se, portanto, uma alteração de paradigma e uma "ressignificação de conceitos, marcada pelo fluxo informacional em massa, abrangendo-se novas nuances sobre o direito ao segredo, o direito à intimidade, o direito à vida privada e familiar, o direito à autodeterminação informativa e o direito à proteção de dados pessoais" (Pessoa, 2020, p. 85). Com esta nova perspectiva, apesar de ter sido anunciado o "fim da privacidade no apagar das luzes do século XX, tenta-se conceituar o direito à privacidade como uma superação da concepção sólida e estática dos textos normativos fechados de autoconfinamento para alcançar uma perspectiva aberta, dinâmica e fluida numa sociedade tecnológica" (Pérez-Luño, 2012, p. 93).

Quanto à proteção de dados pessoais, percebe-se um longo processo normativo-regulatório, identificado em quatro fases legislativas (Doneda, 2011, p. 96). A primeira fase, considerando o estado da arte da tecnologia, propôs normas que demandavam a autorização e o consentimento do usuário para a criação e manutenção de bancos de dados estruturados, além de regular as funções do poder público no manejo das informações coletadas. A segunda fase, reagindo à crescente utilização de bancos de dados, introduziu regulamentações que concebiam a privacidade como uma liberdade negativa, permitindo, ao titular, limitar ou vetar o acesso do poder público aos seus dados pessoais.

Já na década de 1980, considerando a necessidade de tratamento de dados pessoais dos titulares nos fluxos informativos de uma economia global, a terceira fase legislativa buscou ir além da noção restrita de que autorização ou consentimento fossem suficientes para atividades que envolviam informações pessoais, em referência à autodeterminação informativa. Por último, a quarta fase legislativa, representando o estágio atual, reconhece que a privacidade não pode ser diminuída a uma mera escolha individual, mas deve antecipar a criação de normas coletivas de garantias e direitos para os titulares. Com isso, é possível ir além do consentimento diante das novas possibilidades de processamento de dados e a clara disparidade na relação jurídica entre entidades e usuários, destacando a importância de autoridades independentes para a supervisão pública do processamento de dados na sociedade.

Entretanto, o cenário vigente continua caracterizado por dispositivos cada vez mais intensos de vigilância dos titulares, ou seja, pela coleta e tratamento de dados, sejam eles pessoais ou não, para sustentar essa nova ordem socioeconômica baseada na informação, bem como essa nova estrutura de vigilância descentralizada (Pessoa; Oliveira, 2019, p. 11). A regulamentação do direito à privacidade, na conjuntura legislativa atual, deve levar em conta os fluxos de informação globais e transnacionais, compreendendo os dados como bens econômicos e fontes de receita publicitária, numa nova expressão do capitalismo.

Nota-se uma "necessidade de pensar a regulação em uma sociedade marcada pela vigilância, o que não implica apenas a adoção de dispositivos legais que protejam dados e informações, mas também todo e qualquer instrumento ou técnica que apresente um efeito regulatório" (Rodriguez, 2021, p. 116). É importante mencionar que "a adoção de medidas dessa natureza exige, por vezes, a conivência com algumas formas positivas de vigilância virtual, norteadas por garantias e princípios que digam respeito à tutela das informações transferidas no espaço material e imaterial da sociedade" (Rodriguez, 2021, p. 116).

Nesse contexto, caso a proteção da privacidade fique condicionada aos interesses econômicos e avanços tecnológicos, inclusive baseada numa autorregulação regulada do mercado, cabe perguntar se há verdadeiro comprometimento dos atores estatais e corporativos com a tutela desse direito, uma vez que as redes de poder tendem a eliminar os vácuos e relativizar os limites normativos em favor da publicidade e do lucro (Rodotà, 2008, p. 105). Dessa forma, relegar a proteção e dados à autorregulação ou a nenhuma regulação pode acabar por considerar a privacidade como simples *commodity* no mercado globalizado e de exploração de ativos econômicos de vigilância, o que não se coaduna com a tutela dos direitos fundamentais da personalidade humana.

A evolução dos marcos regulatórios, que culmina na concepção e implementação de legislações de proteção de dados, traz à tona a definição dos princípios e direitos garantidos que devem ser assegurados aos titulares dos dados. Esses princípios são a espinha dorsal de uma regulamentação eficaz, orientando a atuação de entidades públicas e privadas, bem como assegurando que os interesses dos cidadãos sejam preservados em um ambiente digital cada vez mais intrusivo.

Os direitos garantidos por estas leis geralmente incluem, mas não se limitam, ao direito de acesso, retificação, exclusão e portabilidade de dados, bem como o direito de contestar decisões automatizadas e de ser informado sobre coletas e usos dos dados. A inclusão de princípios, como a minimização de dados, limitação de finalidade, e a transparência nas operações de dados assegura que as entidades que processam dados não apenas cumpram

com as obrigações legais, mas também adotem uma postura ética e responsável. Desse modo, esses princípios constituem, atualmente, como entendimento comum, a base para o exercício da autonomia digital, permitindo que os indivíduos tenham controle sobre suas informações pessoais e se protejam contra usos indevidos, numa lógica de "pessoa-informação-controle-circulação" (Rodotà, 2008, p. 93).

Nesse contexto, cabe fazer especial referência ao 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 e que revoga a Diretiva 95/46/CE. Conhecido por Regulamento Geral sobre a Proteção de Dados ou pela sigla RGPD, ele introduz um novo regime jurídico sobre proteção de dados pessoais na União Europeia, demandando uma postura proativa, consciente, diligente e responsável do agente de tratamento. Essa postura deve ser baseada na avaliação e mitigação do risco e na adoção de medidas de segurança administrativas e técnicas para tutelar o titular de direitos, enfocando também nas boas práticas e políticas de privacidade (União Europeia, 2016).

Ocorre que o RGPD acaba por superar os limites territoriais da União Europeia, porque traz hipóteses de aplicação independentemente do local de tratamento dos dados, da nacionalidade do titular ou da sede do agente de tratamento. O RGPD fez com que vários países fora do bloco se vissem diante da necessidade de adequação das normativas nacionais aos padrões europeus, fortalecendo, ainda mais, o fenômeno denominado "Europeização" ou "Efeito Bruxelas" (Bradford, 2012). Isso, porque, por exemplo, o RGPD previu medidas de cooperação internacional e restrições ao fluxo transfronteiriço de dados. Estabeleceu-se, então, que a União Europeia concederia decisão de adequação ou conformidade a países de fora do bloco, que possuem um nível adequado de proteção de dados pessoais para manutenção das práticas comerciais com a região e para realização de transferências internacionais (Pessoa; Limberger; Saldanha, 2023).

Trata-se de um duplo viés, uma vez que a regulação da proteção de dados pessoais "por um lado, procura proteger a pessoa física em relação ao tratamento de seus dados pessoais, por outro se destaca sua missão de induzir o comércio mediante o estabelecimento de regras comuns para proteção de dados na região". No entanto, no caso, "as exigências de um mercado unificado como o europeu em diminuir de forma ampla os custos de transações inclui harmonizar as regras relativas a dados pessoais" no globo, especialmente em razão da importância do bloco (Doneda, 2011, p. 102).

A construção de mecanismos de fiscalização e a imposição de sanções, como previsto nos marcos regulatórios de proteção de dados, evidenciam a seriedade e o compromisso de um ordenamento jurídico com o direito à proteção de dados pessoais. No entanto, quando essas estruturas normativas são exportadas para além de suas fronteiras originais, surge a problemática do imperialismo regulatório. Com a adoção do Regulamento Geral de Proteção de Dados Pessoais, como referência internacional, a União Europeia posiciona-se, mais uma vez, como exportadora de padrões regulatórios, o que pode ser interpretado como uma forma de extensão da sua influência geopolítica.

Este fenômeno de projeção normativa não é desprovido de críticas, especialmente quando considerado sob a ótica das nações que se encontram na periferia do capitalismo de dados. A adoção de regulamentos estrangeiros muitas vezes é feita sem a necessária adaptação ao contexto local, podendo resultar em normas desajustadas que não refletem as necessidades e particularidades de outras sociedades. Isso pode levar a uma situação paradoxal em que, ao invés de empoderar os usuários de dados, a regulamentação acaba por reforçar a dependência tecnológica e normativa.

A ideia de imperialismo regulatório também remete à discussão sobre o equilíbrio de poder no âmbito da governança global de dados. Enquanto o Regulamento Geral de Proteção de Dados Pessoais oferece um modelo abrangente de direitos e proteções aos residentes da União Europeia, sua adoção como um modelo global pode restringir a capacidade de inovação regulatória em outras regiões e perpetuar uma dinâmica de centro-periferia. Desse modo, os países centrais definem as regras que os países periféricos devem seguir em novas formas de colonialismo (Silveira, 2021, p. 33-52).

No contexto de um imperialismo regulatório, a adaptação e as resistências locais surgem como contrapontos essenciais. Essas dinâmicas revelam a capacidade e o esforço dos países em desenvolver uma interpretação própria das normas internacionais ou, ainda que nacionais ou comunitárias, que extrapolaram os limites da territorialidade, ajustando-as às realidades sociopolíticas, econômicas e culturais locais. Trata-se de um processo emblemático da luta para manter a soberania nacional na era digital, reforçando-se a necessidade de uma governança de dados que seja tanto globalmente informada quanto localmente enraizada.

3 Sobre o colonialismo digital e a emancipação do direito à proteção de dados pessoais

A livre circulação de dados pessoais é condição para o funcionamento dos produtos e serviços baseados em dados, permitindo que as *big techs,* tais como Google, Facebook, Apple etc., floresçam em um mercado sem fronteiras, capitalizando massivamente os valores gerados pelo fluxo contínuo e irrestrito de informações no globo, razão pela qual se menciona a existência de um capitalismo de plataforma (Srnicek, 2016; Van Dijck, Poell, De Waal, 2018). Esta era digital, muitas vezes referida como a "nova economia do petróleo", viu os dados se transformarem em uma *commodity* essencial para a sustentação e crescimento econômico das gigantes tecnológicas (Zuboff, 2019, p. 14-15).

Além disso, a valorização dos dados pessoais e sua transformação em ativos econômicos traz à tona questões de distribuição de riqueza e equidade social. A disparidade entre os que geram os dados e os que efetivamente se beneficiam de seu valor econômico reflete e intensifica as desigualdades preexistentes na sociedade. O capitalismo de dados, em sua forma atual, parece favorecer uma acumulação desproporcional de capital pelas corporações que têm a capacidade e os recursos para processar e monetizar essas informações (Cassino, 2021, p. 13-32).

O controle sobre os dados pessoais, por sua vez, implica não apenas na capacidade de influenciar o comportamento do mercado e as tendências econômicas, mas também na possibilidade de moldar discursos, opiniões e, em última instância, a própria democracia (Han, 2022, p.8-10). O tratamento dos dados pessoais como uma *commodity* possui implicações profundas para a autodeterminação informativa, onde a capacidade de controlar a própria informação pode ser uma grande falácia discursiva (Pessoa, 2020, p. 92-95).

Nesse contexto, a implementação de leis e normas de proteção de dados, embora essenciais para a salvaguarda da privacidade, podem inadvertidamente consolidar o poder das entidades que já operam com vantagem significativa no espaço digital e na economia de dados. A questão central é como as políticas de proteção de dados, ao invés de democratizar o controle sobre a informação, podem acabar por consolidar desigualdades existentes, inclusive porque, muitas vezes, a legislação vem acompanhada de intenso *lobby* para beneficiar as grandes corporações.

Pontua-se que, para alguns, as estruturas regulatórias têm o potencial de criar barreiras de entrada no mercado de dados, favorecendo conglomerados tecnológicos já estabelecidos que possuem recursos para navegar no complexo ambiente legal e técnico (Silveira, 2021, p. 33-52). Estas corporações, armadas com infraestruturas avançadas e capitais robustos, podem se adaptar mais facilmente às exigências regulatórias, enquanto *startups* e pequenas empresas enfrentam desafios significativos, o que não apenas reforça a posição dominante de grandes *players*, mas também limita a inovação e a competição, fatores essenciais para um mercado sustentável.

Na medida em que as regulamentações são mais estritas em algumas regiões do que em outras, verifica-se uma tendência de centralização da indústria de dados em locais com regimes regulatórios mais permissíveis ou com infraestruturas mais desenvolvidas, enquanto que a exploração de dados ocorre por todo o globo (Faustino; Lippold, 2023; Silveira, 2021; Cassino, 2021). Tal fenômeno não só reforça a hegemonia de certos países e regiões, mas também pode levar a uma nova forma de dependência digital para aqueles que se encontram fora desses polos tecnológicos.

O paradoxo reside no fato de que a regulação, embora concebida para proteger os usuários, pode, no capitalismo de dados, inadvertidamente, consolidar o poder das *big techs* ao legitimar a coleta de dados sob determinadas condições ou com base em suposto consentimento livre e esclarecido. Em outras palavras, a complexidade da regulação de proteção de dados pode, contra suas escritas intenções, reforçar as estruturas do capitalismo de dados, especialmente em um contexto global baseado na livre circulação de dados, inclusive transferência internacional de ativos digitais.

A transformação do paradigma "pessoa-informação-sigilo" para "pessoa-informação-controle-circulação", especialmente representada pelo advento do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia e outras legislações semelhantes, representou um marco na tentativa de regulamentar o tratamento de dados pessoais. Contudo, apesar de seu potencial emancipatório e fonte de inspiração para levar o protagonismo ao usuário, tais regulamentações podem, na prática, endossar o modelo de acumulação de dados ao impor requisitos que são facilmente absorvidos e contornados pelas corporações dominantes, reforçando, assim, sua posição no mercado.

As regulações atuais, mesmo quando rigorosas, podem falhar em desmantelar as infraestruturas de poder que possibilitam esse modelo econômico. A coleta de dados, quando permitida sob certas condições regulatórias, como

o consentimento informado, pode ser interpretada pelas empresas como um aval para continuar suas operações, agora com a chancela de conformidade legal, já que os termos e condições são verdadeiros contratos de adesão, sequer lidos ou compreendidos pelos usuários (Sujeito a termos [...], 2013).

Na verdade, apesar da regulação tratar os usuários como "titulares" de dados, podem reforçar o poder das *big techs* ao não abordar a questão da propriedade dos dados. As regulamentações se concentram, muitas vezes, na ideia de respeito à privacidade e na proteção de dados pessoais, trazendo o usuário para "participar" desse processo, sem questionar quem, em última análise, detém a propriedade – e, consequentemente, a exploração econômica e os lucros – sobre essas informações e como essa concentração de poder econômico afeta a competição e a inovação (Morozov, 2018, p. 146-147).

Além disso, a transferência internacional de dados, elemento-chave na consolidação do capitalismo de dados, é frequentemente abordada pelas regulamentações, de maneira que reforça esse fenômeno, uma vez que permitem a livre circulação desses ativos, inclusive sem o consentimento do titular, desde que para países com níveis adequados de proteção de dados – leia-se, regulações equivalentes –, ou cumpridas determinadas condições, como a criação de cláusulas-padrão contratuais específicas e normas corporativas globais, dentre outras.

Nesse contexto, emerge a questão do colonialismo de dados, à medida em que as regulações muitas vezes não levam em conta as assimetrias entre países no que diz respeito à capacidade de coletar, processar e monetizar dados. Isso pode resultar em uma forma de colonialismo digital onde as nações mais ricas impõem suas regras e extraem valor dos dados gerados nos países em desenvolvimento, exacerbando as desigualdades existentes (Faustino; Lippold, 2023; Silveira, 2021; Cassino, 2021).

O fenômeno do colonialismo digital no Sul Global é uma das facetas mais problemáticas da economia de dados contemporânea. Nessa linha, a dinâmica entre as nações desenvolvidas do Norte e as em desenvolvimento do Sul estabelece uma forma de neocolonialismo, onde os dados se tornam o novo terreno de exploração e dominação. As corporações do Norte, muitas vezes representadas pelas *big techs*, têm a capacidade e o poder para extrair valor dos dados gerados pelos usuários do Sul Global, perpetuando as desigualdades históricas e criando novas formas de dependência econômica e tecnológica (Harari, 2024, p. 485-491).

O conceito de colonialismo de dados é crucial para entender o extrativismo digital, considerado como uma continuação das práticas coloniais, em que as *big techs* não apenas coletam vastas quantidades de dados, mas também controlam o poder de processá-los e monetizá-los, o que ocorre, frequentemente, sem oferecer compensação justa ou contribuir para o desenvolvimento local, criando um cenário em que os países do Sul Global são meros fornecedores de matéria-prima digital para ser refinada pelas economias avançadas. Este conceito descreve uma realidade onde grandes conglomerados tecnológicos atuam como verdadeiros garimpeiros digitais, explorando dados pessoais como se fossem recursos naturais inesgotáveis, sem a devida consideração pelas implicações éticas ou pelo esgotamento das reservas de privacidade.

No cenário de recrudescimento do capitalismo de vigilância como uma nova lógica de acumulação que se baseia na previsão e modificação do comportamento humano, os dados do Sul Global tornam-se instrumentos para aprimorar algoritmos e tecnologias que, paradoxalmente, muitas vezes não estão disponíveis ou são inacessíveis para as populações locais, exacerbando a desigualdade tecnológica e econômica. Na economia de dados, as assimetrias também são evidentes, já que "os produtores de tecnologia pouco se importam com os consumidores do Sul Global, salvo o recebimento de *feedback* para melhorias de seus próprios produtos ou com alguns nichos lucrativos" (Cassino, 2021, p. 29).

O colonialismo digital, neste sentido, transforma os dados em um recurso altamente desejável e controlável, cujo acesso e uso são determinados por um pequeno número de atores poderosos, predominantemente localizados no hemisfério norte. Por outro lado, a assimetria informacional reforça a mentalidade de alienação técnica, em que existe uma "ignorância ativa sobre como funcionam as redes de criação, desenvolvimento e uso de tecnologias, na fé da completa ausência de importância de se conhecer e dominar localmente os processos tecnológicos" (Silveira, 2021, p. 45).

Nesse contexto, algumas questões são ofuscadas pela mentalidade colonial, tais como: a "dúvida sobre a crença de que as empresas e plataformas digitais são neutras e que não interferem em nosso cotidiano, exceto para nos servir"; ainda, "a interrogação sobre a inexistência de consequências negativas locais e nacionais na utilização das estruturas tecnológicas das plataformas, uma vez que elas respeitariam os contratos"; também "a avaliação de que as implicações sobre a coleta massiva de dados nos países centrais da plataformização tecnológica possuem

os mesmos efeitos econômicos, políticos e socialmente moduladores que nos países periféricos"; bem como "a indagação sobre se seria possível apostar no avanço de uma inteligência computacional local, na soberania algorítmica e no conhecimento tecnológico como um bem comum livre" (Silveira, 2021, p. 36).

O colonialismo digital é alimentado por um modelo de negócios que vê os dados não apenas como um ativo, mas como um recurso primordial para o desenvolvimento de novos produtos, serviços e obtenção de vantagens competitivas. A coleta massiva de dados torna-se um imperativo corporativo, onde o consentimento dos usuários é frequentemente reduzido a uma mera formalidade (Pessoa, 2018, p. 92). Esse processo de captação contínua de informações detalhadas sobre comportamentos, preferências e relações sociais transforma a experiência humana em uma mercadoria, uma fonte de lucro.

A relação entre a extração de dados e o poder econômico é reforçada pelo "deslumbre" tecnológico e pela aparente gratuidade da inovação, muitas vezes mascarando as assimetrias e explorações inerentes à economia de dados. Dessa forma, a infraestrutura da internet e das plataformas digitais, controlada pelas *big techs*, favorece uma distribuição desigual dos benefícios gerados pelo tráfego global de dados, uma vez que, enquanto os indivíduos geram os dados que alimentam as máquinas de lucro das corporações, eles raramente participam dos benefícios econômicos resultantes dessa exploração.

Essa dinâmica do colonialismo digital também reflete e amplia desigualdades geopolíticas. Os países do Sul Global, muitas vezes com regulamentações menos rigorosas e infraestruturas tecnológicas em desenvolvimento ou com a implementação de regulações de proteção de dados inspiradas em contextos do Norte Global, tornam-se territórios férteis para a exploração de dados por empresas situadas nos centros de poder econômico e tecnológico globais, acabando por perpetuar padrões históricos de exploração e subjugação.

A extração de dados pode ser vista como uma extensão das práticas coloniais que buscam não apenas recursos materiais, mas também intelectuais e culturais, visando a homogeneização e a imposição de valores e sistemas de crença (Fanon, 2005, p. 55-56). Esse desequilíbrio reforça a necessidade de reexaminar os modelos de negócios dominantes no setor tecnológico, buscando fórmulas que compartilhem de forma mais justa os frutos do mundo digital com aqueles que fornecem a matéria-prima consubstanciada nos dados pessoais (Faustino, 2023, p. 53-55).

A análise da inovação tecnológica como um contraponto ao colonialismo digital conduz a considerar a relevância da legislação de proteção de dados. Nesse cenário, o Regulamento Geral de Proteção de Dados da União Europeia parece chancelar esse colonialismo digital, quando reconhece que a livre circulação de dados pessoais no interior da União Europeia não é restringida nem proibida por motivos relacionados com a proteção das pessoas no que respeita ao tratamento de dados pessoais (União Europeia, 2016).

Por oportuno, diversos países têm se inspirado na União Europeia para criar seus próprios sistemas de regulação de privacidade, adotando normas parecidas de proteção de dados pessoais. Nesse sentido, o RGPD estabelece, dentre os requisitos para ocorrer o fluxo transfronteiriço de dados pessoais, a necessidade de decisão de nível adequado de proteção de dados, que compete à Comissão Europeia, inspirando diversos países a adotarem o modelo europeu para criação ou atualização de normas de privacidade, tais como o Brasil, Argentina, Uruguai, Nova Zelândia, Japão e, inclusive, China (Pessoa; Limberger; Saldanha, 2023, p. 177-178).

No Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018, marca um avanço significativo na legislação brasileira em relação ao direito à proteção de dados pessoais. Inspirada pelo Regulamento Geral sobre a Proteção de Dados Pessoais da União Europeia, a LGPD é reflexo dessa influência, constituindo um esforço para alinhar o país com as práticas internacionais de privacidade e proteção de dados, no contexto do capitalismo de dados (Brasil, 2018).

Contudo, embora represente o marco fundamental de um regime jurídico do direito à proteção de dados pessoais, que tenta trazer protagonismo ao usuário sobre o controle de suas informações, é preciso analisar a LGPD também de forma crítica (Sarlet, 2021, p. 16-22). Apesar da comemoração e do entusiasmo por parte de alguns setores quanto à inspiração no modelo europeu de regulação de proteção de dados, elevando o Brasil a uma posição de garante da privacidade, a LGPD enfrenta desafios únicos, decorrentes do contexto socioeconômico e das desigualdades estruturais existentes no país, não apenas relacionados aos problemas de privacidade e tecnologia, porém também questões mais amplas do capitalismo de dados e do colonialismo digital.

No contexto do Sul Global, a evolução dos marcos regulatórios precisa considerar o risco de implementar regulamentações descontextualizadas, que não levam em conta as particularidades da região (Dussel, 2009). A

busca por um equilíbrio entre a adaptação de melhores práticas internacionais e a criação de soluções inovadoras que atendam às necessidades locais é um desafio premente, tornando-se necessário questionar como a evolução dos marcos regulatórios pode influenciar não apenas a proteção e o tratamento de dados pessoais, mas também o poder e o controle que os indivíduos possuem sobre suas informações digitais.

O desafio para os países do Sul Global é, portanto, duplo: por um lado, devem buscar a proteção dos dados pessoais de seus cidadãos, o que muitas vezes significa alinhar-se aos padrões internacionais, normas corporativas globais e padrões técnicos comuns; por outro lado, devem manter sua soberania e a capacidade de promover o desenvolvimento econômico e tecnológico de acordo com seus próprios termos, sem sucumbir à pressão de se conformar a um modelo que pode não ser totalmente adequado às suas realidades.

A cooperação Sul-Sul também desempenha um papel vital neste contexto, possibilitando que países em desenvolvimento compartilhem conhecimentos, experiências e estratégias para a proteção de dados e a privacidade. Este intercâmbio pode fortalecer a posição de tais países nas negociações internacionais e na formulação de políticas, além de fomentar uma visão alternativa que contraste com a narrativa dominante do Norte Global. Através da lente das necessidades e particularidades locais, as políticas de dados podem ser reformuladas para capacitar os cidadãos, estimular o crescimento de tecnologias nativas e promover um ecossistema digital que seja inclusivo e representativo.

Resistir ao modelo de regulação de dados imposto externamente não significa rejeitar os valores subjacentes à proteção de dados e à privacidade. Pelo contrário, significa engajar-se em um diálogo crítico com esses modelos, questionando e reformulando-os de maneira que alavanquem as capacidades locais e promovam a autonomia digital. Portanto, o direito à proteção dos dados pessoais no capitalismo de dados e no colonialismo digital não é apenas um fenômeno econômico, mas também uma questão de justiça social e direitos humanos.

O direito à proteção de dados pessoais, enquanto conceito jurídico e prática regulatória, adquiriu contornos globais, influenciados principalmente por modelos desenvolvidos no Norte Global, como o RGPD da União Europeia. No entanto, ao considerar os países do Sul Global, é imprescindível reconhecer que a mera importação de estruturas regulatórias concebidas em realidades distintas pode não ser suficiente para endereçar as especificidades locais e os desafios impostos pelo capitalismo de dados e pelo colonialismo digital (Pessoa, Limberger, Saldanha, 2023, p. 177-179).

Pode-se explorar a necessidade de emancipação do direito à proteção de dados pessoais nos países do Sul Global a partir de uma abordagem decolonial e contextualizada dos avanços tecnológicos. Esta noção propõe que o direito à proteção de dados deve ser transformado para refletir as dinâmicas socioeconômicas, políticas e culturais próprias desses países, de modo que, em vez de ser um conceito importado e imposto, deve evoluir para se tornar um instrumento de empoderamento e autonomia.

A emancipação do direito à proteção de dados, portanto, envolve a criação de marcos regulatórios que não somente protejam os indivíduos contra abusos na coleta e uso de seus dados, mas que também promovam a soberania digital dos países do Sul Global. Isso significa desenvolver políticas que permitam o controle desses países sobre seus dados, assegurando que sejam utilizados de maneira a beneficiar suas próprias sociedades e economias, e não apenas as corporações estrangeiras ou os interesses do Norte Global.

Nesse sentido, o direito à proteção de dados no Sul Global deve ser visto como um direito dinâmico e adaptável, capaz de resistir às pressões do colonialismo digital e de responder às expressões de desigualdades sociais geradas pelo capitalismo de dados. Isso requer uma perspectiva crítica que questione os pressupostos subjacentes aos modelos regulatórios importados e que busque, através do direito, uma forma de reequilibrar o poder na economia de dados global.

4 Conclusão

A emergência do capitalismo de dados representa um fenômeno marcante na era digital contemporânea, reconfigurando o paradigma através do qual informações pessoais são reguladas, compartilhadas, tratadas e capitalizadas. A análise crítica deste artigo permitiu uma imersão compreensiva nos meandros de um sistema que, sob a inspiração de modelos regulatórios como o Regulamento Geral de Proteção de Dados da União Europeia, pode inadvertidamente alimentar dinâmicas de poder desequilibradas, caracterizando um possível neocolonialismo digital.

Percebe-se o nascimento e consolidação de um capitalismo de dados sob o domínio das *big techs*, baseado na coleta, tratamento, compartilhamento e comercialização de informações pessoais, que escapa da construção dos modelos regulatórios de proteção de dados pessoais. Identificou-se que o padrão europeu, representado pelo Regulamento Geral de Proteção de Dados da União Europeia, que serve de inspiração para outras regulações ao redor do globo, apesar de suas intenções de proteger o indivíduo, pode não considerar inteiramente as complexidades e necessidades de contextos distintos, como os dos países do Sul Global.

Dessa forma, o atual modelo de regulação, com forte influência do Regulamento Geral de Proteção de Dados da União Europeia, com seu foco na livre circulação de dados, reforça e dá legitimidade ao capitalismo de dados, haja vista que o controle sobre os dados pessoais por parte dos titulares é uma ilusão diante da economia digital capitalizada pelas *big techs*. A análise da Lei Geral de Proteção de Dados do Brasil destacou como tal legislação, embora siga a tendência europeia, apresenta uma oportunidade de reflexão e adaptação às realidades locais, especialmente frente ao colonialismo digital.

Em outras palavras, observa-se que a regulação brasileira sobre o direito à proteção de dados pessoais, ao espelhar-se no regulamento europeu, corre o risco de ecoar as práticas de capitalismo de dados e de colonialismo digital. No entanto, essa adoção não é um caminho sem retorno, já que a LGPD pode abrir espaço para uma interpretação que pode transcender a imitação, promovendo um diálogo mais equilibrado entre proteção de dados pessoais e realidades socioeconômicas.

Trata-se da necessidade de uma visão decolonial que resgate a autonomia e fomente a soberania digital dos países do Sul Global. Dessa forma, é possível explorar uma emancipação do direito à proteção de dados pessoais, que surge não apenas como um desafio, mas como uma imperativa ação para garantir que a privacidade opere como um verdadeiro instrumento de empoderamento social e econômico, resistindo às pressões do capitalismo de dados e às novas expressões de um colonialismo digital.

Referências

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Rio de Janeiro: Jorge Zahar, 2013.

BRADFORD, Anu. The Brussels Effect. **NorthWestern University Law Review**, [*s. l.*], v. 107, n. 1, p. 1-68, 2012. Disponível em: https://scholarship.law.columbia.edu/faculty_scholarship/271. Acesso em: 10 dez. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 13 dez. 2023.

CASSINO, João Francisco. O sul global e os desafios pós-coloniais na era digital. *In*: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da. **Colonialismo de dados:** como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia literária, 2021. p. 13-32.

DONEDA, Danilo. A proteção de dados pessoais como um direito fundamental. **Espaço Jurídico,** Chapecó-SC, v. 12, n. 2, p. 91-110, jul./dez., 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315. Acesso em: 01 dez. 2023.

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

DUSSEL, Enrique. Meditações anti-cartesianas sobre a origem do anti-discurso filosófico da modernidade. *In*: SANTOS, Boaventura de Sousa; MENESES, Maria Paula. **Epistemologias do Sul.** Coimbra: Edições Almedina, 2009. p. 283-336.

FANON, Frantz. **Os condenados da terra.** Juiz de Fora: UFJF, 2005.

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

HAN, Byung-Chul. **Infocracia**: digitalização e a crise da democracia. Petrópolis: Vozes, 2022.

HARARI, Yuval Noah. **Homo Deus**: uma breve história do amanhã. São Paulo: Schwarcz, 2015.

HARARI, Yuval Noah. **Nexus**: uma breve história das redes de informação, da Idade da Pedra à inteligência artificial. São Paulo: Companhia das Letras, 2024.

HOCH, Patrícia Adriani; ENGELMANN, Wilson. Regulação da inteligência artificial no Judiciário brasileiro e europeu. **Pensar, Revista de Ciências Jurídicas**, Fortaleza, v. 28, n. 4, p. 1-18, out./dez. 2023. DOI: https://doi.org/10.5020/2317-2150.2023.14263

HUI, Yuk. **Tecnodiversidade**. São Paulo: Ubu, 2020.

LIMBERGER, Têmis. Da evolução do direito de ser deixado em paz à proteção dos dados pessoais. **Novos Estudos Jurídicos,** Itajaí, v. 14, n. 2, p. 27-53, 2009. Disponível em: https://periodicos.univali.br/index.php/nej/article/view/1767/1407. Acesso em: 13 dez. 2023.

MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. In: AGRE, Phillip; ROTENBERG, Marc (org.). **Technology and privacy**: The new landscape. Cambridge: MIT Press, 1997. Chapter 8. *E-book*. DOI: https://doi.org/10.7551/mitpress/6682.003.0010

MOROZOV, Evgeny. **Big Tech.** São Paulo: Ubu, 2018.

O'NEIL, Cathy. **Algoritmos de destruição em massa:** como o *big data* aumenta a desigualdade e ameaça à democracia. Santo André: Rua do Sabão, 2020.

PÉREZ-LUÑO, Antonio Enrique. **Los derechos en la sociedad tecnológica.** Madri: Editorial Universitas, S.A., 2012.

PÉREZ-LUÑO, Antonio-Enrique. **Derechos humanos, Estado de Derecho y Constitución.** 9. ed. Madri: Editorial Tecnos, 2005.

PESSOA, João Pedro Seefeldt Pessoa; LIMBERGER, Têmis; SALDANHA, Jânia Maria Lopes. A proteção de dados pessoais entre capitalismo de vigilância e cosmopolitismo. **Revista da Faculdade Mineira de Direito,** Belo Horizonte, v. 26, n. 52, p. 156-185, 2023. Disponível em: https://periodicos.pucminas.br/index.php/Direito/article/view/30789. Acesso em: 27 dez. 2023.

PESSOA, João Pedro Seefeldt Pessoa; OLIVEIRA, Rafael dos Santos de. "Big Brother Watch and Others v. The United Kingdom": el regimen de vigilancia social y el derecho al respect a la vida privada y familiar y a la libertad de expresión frente a la Corte Europea de Derechos Humanos. **Pensar, Revista de Ciências Jurídicas**, Fortaleza, v. 24, n. 3, pp. 1-12, jul./set. 2019. DOI: https://doi.org/10.5020/2317-2150.2019.9528

PESSOA, João Pedro Seefeldt. **O Efeito Orwell na sociedade em rede:** cibersegurança, regime global de vigilância social e direito à privacidade no século XXI. Porto Alegre: Fi, 2020. Disponível em: https://www.editorafi.org/073orwell. Acesso em: 02 dez. 2023.

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

RODRIGUEZ, Daniel Piñero. **O direito fundamental à proteção de dados:** vigilância, privacidade e regulação. Rio de Janeiro: Renovar, 2021.

SANTOS, Boaventura de Sousa. Para além do pensamento abissal: das linhas globais a uma ecologia dos saberes. In: SANTOS, Boaventura de Sousa; MENESES, Maria Paula. **Epistemologias do Sul**. Coimbra: Edições Almedina, 2009. p. 23-72.

SARLET, Ingo Wolfgang. O direito fundamental à proteção de dados pessoais na Constituição Federal Brasileira de 1988. **Revista Privacidade e Proteção de Dados,** [*s. l.*], v. 1, n. 1, p.1-49, 2021. Disponível em https://repositorio.pucrs.br/dspace/handle/10923/18868. Acesso em: 13 dez. 2023.

SILVEIRA, Sérgio Amadeu da. A hipótese do colonialismo de dados e o neoliberalismo. In: CASSINO, João Francisco; SOUZA, Joyce; SILVEIRA, Sérgio Amadeu da (org.). **Colonialismo de dados:** como opera a trincheira algorítmica na guerra neoliberal. São Paulo: Autonomia literária, 2021. p. 33-52.

SILVEIRA, Sergio Amadeu da. **Democracia e os códigos invisíveis***:* como os algoritmos estão modulando comportamentos e escolhas políticas. São Paulo: Edições Sesc São Paulo, 2019.

SRNICEK, Nick. **Platform Capitalism**. Cambridge: Polity Press, 2016.

SUJEITO A TERMOS e condições. Direção de Cullen Hoback. Nova Iorque: Variance Films; Hyrax Films, 2013. (80 min.), son., color.

UNIÃO EUROPEIA. Parlamento Europeu, Conselho da 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **European Union law,** Luxembourg, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A32016R0679. Acesso em: 12 dez. 2023.

VAN DIJCK, José; POELL, Thomas; DE WAAL, Martijn. **The platform society:** Public values in a connective world. Reino Unido: Oxford University Press, 2018.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância.** Rio de Janeiro: Intrínseca, 2019.

ZUBOFF, Shoshana. Big Other: capitalismo de vigilância e perspectivas para uma civilização de informação. *In*: BRUNO, Fernanda; CARDOSO, Bruno; KANASHIRO, Marta; GUILHON, Luciana; MELGAÇO, Lucas (Org.). **Tecnopolíticas da vigilância:** perspectivas da margem. São Paulo: Boitempo, 2018, p. 17-68.