REVISTA ESMAT 28

CAPITALISMO DE VIGILÂNCIA E SOCIEDADE BRASILEIRA: ANÁLISE CRÍTICA E JURISPRUDENCIAL A PARTIR DE SHOSHANA ZUBOFF

SURVEILLANCE CAPITALISM AND BRAZILIAN SOCIETY: A CRITICAL AND JURISPRUDENTIAL ANALYSIS BASED ON SHOSHANA ZUBOFF

Anderson Filipini Ribeiro[1]
Filipe Mello Sampaio Cunha[2]
Natalia Maria Ventura da Silva Alfaya[3]

RESUMO

Este artigo analisa criticamente a teoria do capitalismo de vigilância desenvolvida por Shoshana Zuboff, articulando-a com a realidade brasileira contemporânea. O problema central investigado reside na forma como a extração massiva de dados pessoais, impulsionada por grandes corporações tecnológicas, afeta direitos fundamentais no Brasil, aprofundando desigualdades sociais e comprometendo a soberania informacional do país. O objetivo principal é examinar como o capitalismo de vigilância se manifesta no contexto brasileiro, especialmente em relação à desigualdade digital, à utilização de tecnologias de reconhecimento facial pelo Estado, à gestão de dados

1 Mestrando em Direito, pelas Faculdades Londrina. Bacharel em Direito e Teologia. Pós-Graduado em Direito Penal, Direito Militar, Administração e Segurança Pública, e em Direito Civil e Processual Civil. Habilitações linguísticas, nível B1, nos idiomas: Espanhol (DELE), Francês (DELF) e Italiano (CILS). Lattes: http://lattes.cnpq.br/0703783803020290. E-mail: direito.andersonfilipini@gmail.com https://orcid.org/0009-0008-5145-2476

2 Mestrando em Direito, pelas Faculdades Londrina. Bacharel em Direito e Ciências Políticas. Pós-Graduado em Gestão Pública, Gestão de Processos BPM-CBOK, bem como Gestão das Águas e Sustentabilidade dos Recursos Hídricos no Brasil. Lattes: http://lattes.cnpq.br/4680398321828617. E-mail: filipemgm@gmail.com

3 Graduada em Direito, pela Universidade Estadual de Londrina, 2005-2009. Especialista em Direito Internacional e Econômico, 2010-2011; e em Filosofia Jurídica, 2020-2021, ambas pela Universidade Estadual de Londrina. Mestra em Direito Negocial, pela Universidade Estadual de Londrina, 2012-2014. Doutora em Ciências Jurídicas e Sociais do Programa de Pós-Graduação em Sociologia e Direito, pela Universidade Federal Fluminense, 2015-2018. Advogada inscrita na OAB/PR 59.792. Docente do curso de graduação em Direito da Escola de Direito das Faculdades Londrina (EDFL) e do Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias, pela mesma IES. Lattes: http://lattes.cnpq.br/9731930696524695. E-mail: naty.alfaya@gmail.com https://orcid.org/0000-0002-0312-3677

sensíveis em políticas públicas e aos desafios jurídicos para a proteção da privacidade. A metodologia adotada é de natureza teórico-conceitual e exploratória, com revisão bibliográfica das principais obras sobre o tema – destacando-se Zuboff (2019) – e análise de jurisprudência brasileira, especialmente decisões paradigmáticas do Supremo Tribunal Federal (ADI 6.387 e ADI 5.527) e do Superior Tribunal de Justiça sobre proteção de dados. Nas considerações finais, conclui-se que o Brasil enfrenta desafios específicos na contenção das práticas do capitalismo de vigilância, devido à combinação de desigualdades estruturais, dependência tecnológica e fragilidades institucionais. Contudo, também se observa a emergência de resistências importantes, tanto no campo regulatório – com a promulgação da LGPD e a atuação da ANPD – quanto na atuação do Judiciário e da sociedade civil. O artigo aponta a necessidade de fortalecer políticas públicas, regulamentações e movimentos sociais para garantir a proteção de direitos fundamentais na era digital.

PALAVRAS-CHAVE: Capitalismo de Vigilância. Proteção de Dados. Brasil. Jurisprudência. Shoshana Zuboff.

ABSTRACT

This article critically analyzes the theory of surveillance capitalism developed by Shoshana Zuboff, articulating it with the contemporary Brazilian reality. The central problem investigated lies in how the massive extraction of personal data, driven by large technological corporations, affects fundamental rights in Brazil, deepening social inequalities and compromising the informational sovereignty of the country. The main objective is to examine how surveillance capitalism manifests in the Brazilian context, especially in relation to digital inequality, the use of facial recognition technologies by the state, the management of sensitive data in public policies, and the legal challenges for the protection of privacy. The adopted methodology is of a theoretical-conceptual and exploratory nature, with a literature review of the main works on the subject – highlighting Zuboff (2019) – and analysis of Brazilian jurisprudence, especially paradigm decisions from the Supreme Federal Court (ADI 6.387 and ADI 5527) and the Superior Court of Justice regarding data protection. In the final considerations, it is concluded that Brazil faces specific challenges in containing the practices of surveillance capitalism, due to the combination of structural inequalities, technological dependency, and institutional weaknesses. However, there is also an observation of the emergence of significant resistances, both in the regulatory field – with the enactment of the LGPD and the actions of the ANPD – and in the Judiciary's and civil society's actions. The article highlights the need to strengthen public policies, regulations, and social movements to ensure the protection of fundamental rights in the digital age.

KEYWORDS: Surveillance Capitalism. Data Protection. Brazil. Jurisprudence. Shoshana Zuboff.

INTRODUÇÃO

Nas últimas décadas, as transformações impulsionadas pela digitalização têm alterado profundamente a estrutura das sociedades contemporâneas, redefinindo os modos de produção, circulação e consumo de informações. Esse novo cenário é caracterizado por uma intensificação das práticas de coleta, armazenamento e análise de dados pessoais, que passam a desempenhar um papel central nas dinâmicas econômicas e sociais. Shoshana Zuboff (2019), em sua obra seminal "A Era do Capitalismo de Vigilância", identifica nesse processo a emergência de uma nova lógica econômica, que ela denomina de capitalismo de vigilância: um regime que se apropria unilateralmente da experiência humana, convertendo-a em dados comportamentais para fins de previsão, modulação e lucro.

Segundo a autora, esse modelo não apenas explora a informação como recurso estratégico, mas também inaugura uma nova arquitetura de poder, sustentada pela vigilância pervasiva e pela automação algorítmica (Zuboff, 2019). Trata-se de uma transformação qualitativa em relação ao capitalismo industrial, que se pautava na exploração do trabalho e dos recursos naturais, enquanto o capitalismo de vigilância se baseia na extração das subjetividades e das interações cotidianas, transformadas em matéria-prima informacional.

Esse fenômeno adquire contornos especialmente relevantes quando analisado sob a perspectiva do Sul Global, e, em particular, no contexto brasileiro. De acordo com o Relatório TIC Domicílios (2023), aproximadamente 84% dos domicílios brasileiros possuem acesso à internet, o que representa um avanço expressivo em relação à década anterior. Contudo, a qualidade e a intensidade desse acesso revelam profundas assimetrias regionais e socioeconômicas: enquanto nas áreas urbanas a penetração da internet é de 90%, nas zonas rurais não ultrapassa 60%. Além disso, mais de 17 milhões de brasileiros ainda permanecem completamente desconectados, segundo dados do Instituto Brasileiro de Geografia e Estatística (IBGE, 2022).

Essa desigualdade digital tem efeitos diretos na forma como o capitalismo de vigilância se instala e opera no país, pois a extração de dados não é homogênea, mas fortemente condicionada por fatores como renda, escolaridade, raça e localização geográfica. Conforme alerta Canclini (2005), as dinâmicas globais de consumo e comunicação tendem a reproduzir e aprofundar as desigualdades estruturais já existentes, um fenômeno que se manifesta claramente na sociedade brasileira.

A atuação das grandes corporações de tecnologia – as chamadas big techs, como Google, Meta (Facebook, Instagram e WhatsApp), Amazon e TikTok – é central nesse

processo. Essas plataformas, amplamente utilizadas no Brasil, operam com modelos de negócio baseados na monetização de dados comportamentais, empregando complexos sistemas de inteligência artificial para analisar e prever padrões de consumo e comportamento social. No país, o WhatsApp é utilizado por cerca de 98% dos usuários de internet (Datafolha, 2023), consolidando-se não apenas como principal meio de comunicação, mas também como canal privilegiado para a disseminação de desinformação e manipulação política, fenômeno amplamente observado nas eleições de 2018 e 2022.

O problema que motiva esta pesquisa reside na necessidade de compreender como esse modelo econômico – estruturado na extração massiva de dados – afeta os direitos fundamentais no Brasil, especialmente a privacidade, a proteção de dados pessoais, a liberdade individual e a autodeterminação informacional. A Constituição Federal de 1988 assegura, em seu artigo 5º, inciso X, a inviolabilidade da intimidade, da vida privada e da honra, mas a rápida evolução tecnológica criou novas fronteiras e desafios para a efetivação desses direitos (Brasil, 1988).

Em resposta a esses desafios, o Brasil aprovou a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709, de 2018 –, que estabeleceu princípios e regras para o tratamento de dados pessoais, inspirando-se no Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. Mais recentemente, com a promulgação da Emenda Constitucional nº 115, de 2022, a proteção de dados pessoais foi formalmente alçada à categoria de direito fundamental no ordenamento jurídico brasileiro, consagrando uma diretriz constitucional que orienta a atuação dos poderes públicos e das empresas privadas (Brasil, 2018).

Entretanto, como apontam especialistas (Its Rio, 2022; Dados.org, 2023), subsistem importantes lacunas regulatórias e institucionais que fragilizam a eficácia dessas normas, especialmente diante da capacidade de atuação das big techs e da crescente utilização de tecnologias de vigilância pelo Estado, como os sistemas de reconhecimento facial implantados em diversas cidades brasileiras, frequentemente sem adequada fundamentação legal ou controle social.

Nesse sentido, destaca-se o julgamento pelo Supremo Tribunal Federal (STF) da Ação Direta de Inconstitucionalidade (ADI) nº 6.387, na qual se afirmou, de forma categórica, que "o direito à proteção de dados pessoais possui estatura constitucional, sendo condição para o pleno exercício da cidadania" (Brasil, STF, ADI 6.387, Rel. Min. Rosa Weber, 2020). Esta decisão representou um marco na construção da jurisprudência brasileira sobre o tema, reafirmando a centralidade da proteção de dados no sistema de direitos fundamentais.

O objetivo geral deste artigo é analisar criticamente o fenômeno do capitalismo de vigilância a partir da obra de Shoshana Zuboff, articulando-a com a realidade brasileira e refletindo sobre as implicações jurídicas, políticas e sociais desse modelo. Como

objetivos específicos, buscam-se: (i) apresentar os fundamentos teóricos do capitalismo de vigilância; (ii) identificar as tecnologias e arquiteturas que o sustentam; (iii) analisar sua concretização na realidade brasileira, a partir de casos emblemáticos e dados empíricos; (iv) avaliar as respostas institucionais, especialmente as jurídicas, como a LGPD e a atuação do Judiciário; e (v) discutir alternativas de resistência e caminhos para uma governança democrática da tecnologia.

A metodologia adotada é de caráter teórico-conceitual e exploratório, fundamentada na revisão bibliográfica das principais obras e artigos acadêmicos sobre capitalismo de vigilância, proteção de dados, direitos digitais e soberania informacional. Complementarmente, realiza-se uma análise jurisprudencial, com foco em decisões relevantes proferidas pelos tribunais superiores brasileiros, que elucidam como o Direito nacional tem buscado regular e limitar as práticas associadas à vigilância digital, bem como proteger os direitos fundamentais dos cidadãos.

A escolha pelo recorte brasileiro justifica-se pela necessidade de compreender como o capitalismo de vigilância se manifesta em contextos periféricos e desiguais, que apresentam características específicas quanto ao acesso, ao uso e à regulação das tecnologias digitais. Como maior país da América Latina, com uma população superior a 215 milhões de habitantes e com um dos mercados digitais mais dinâmicos do mundo, o Brasil constitui um laboratório privilegiado para o estudo dessas novas formas de poder e dominação, bem como das possibilidades de resistência e de construção de alternativas democráticas (IBGE, 2022; CETIC.br, 2023).

Desse modo, este artigo pretende contribuir para o aprofundamento da reflexão acadêmica sobre as transformações provocadas pelo capitalismo de vigilância, fornecendo subsídios para o debate público e para a formulação de políticas públicas que assegurem a proteção dos direitos fundamentais, a soberania informacional e a promoção de uma sociedade digital mais justa, inclusiva e democrática.

FUNDAMENTOS TEÓRICOS DO CAPITALISMO DE VIGILÂNCIA

Zuboff (2019) define o capitalismo de vigilância como "uma nova ordem econômica que reivindica unilateralmente a experiência humana como matéria-prima gratuita para práticas comerciais ocultas de extração, previsão e venda" (Zuboff, 2019, p. 14). Trata-se de um regime que não apenas coleta dados, mas também transforma a experiência humana em uma fonte de lucro, subordinando o comportamento individual a processos automatizados de modulação e de controle.

O capitalismo de vigilância não é uma simples extensão do capitalismo informacional descrito por Castells (2013), mas uma transformação qualitativa do modo de produção, assentada na captura contínua e massiva de dados comportamentais. Sua

emergência ocorre no seio das grandes empresas de tecnologia, sobretudo Google e Facebook, que inauguram práticas de extração de dados sem precedentes.

Zuboff (2019) introduz o conceito de "dados comportamentais excedentes" para descrever os insumos informacionais que excedem os necessários para melhorar os serviços e são utilizados para gerar novos produtos de previsão comportamental. Esses excedentes alimentam sistemas de inteligência artificial que criam perfis, previsões e, eventualmente, intervenções no comportamento humano.

Essa lógica inaugura um novo ciclo de acumulação de capital, distinto do modelo industrial, baseado na extração de recursos naturais e na exploração do trabalho. Agora, o capital se apropria da subjetividade e das interações humanas, convertendo-as em commodities digitais (Zuboff, 2019).

Zuboff distingue o capitalismo de vigilância de outras formas históricas de poder, ao cunhar os conceitos de "instrumentarianismo" e "Big Other". O instrumentarianismo refere-se à aplicação de instrumentos tecnológicos para a modulação do comportamento, sem necessidade de coerção física direta, mas por meio de arquiteturas digitais persuasivas e imperceptíveis (Zuboff, 2019).

O "Big Other" representa uma nova instância de poder, distinta do "Big Brother" orwelliano, pois atua silenciosamente, coletando e processando dados em tempo real para prever e orientar comportamentos (Zuboff, 2019). Trata-se de uma reconfiguração das relações de poder, em que o controle não se dá pela vigilância ostensiva, mas pela antecipação e pelo condicionamento invisível das ações humanas.

Embora existam paralelos com o panoptismo foucaultiano, o capitalismo de vigilância se distingue pela ausência de uma centralidade disciplinar explícita. Deleuze (1992) já antecipava essa transição ao propor o conceito de "sociedades de controle", no qual o poder opera por modulações contínuas, superando as instituições disciplinares clássicas.

Enquanto o capitalismo industrial visava disciplinar corpos para a produção, o capitalismo de vigilância busca capturar a mente e o comportamento para a predição e à modulação, inaugurando uma nova configuração do poder social (Zuboff, 2019).

A ARQUITETURA TÉCNICA E SOCIAL DA VIGILÂNCIA

A materialização do capitalismo de vigilância depende de um complexo ecossistema tecnológico, que inclui cookies, rastreadores, sensores de Internet das Coisas (IoT), inteligência artificial e sistemas de reconhecimento facial. Essas tecnologias permitem a coleta massiva e contínua de dados, transformando dispositivos cotidianos em instrumentos de vigilância ubíqua (Zuboff, 2019).

No Brasil, o uso de sistemas de reconhecimento facial em espaços públicos tem crescido, especialmente em programas de segurança pública, como no metrô de São Paulo e em sistemas de videomonitoramento em diversas capitais (Dados.org, 2023).

As plataformas digitais, como Google, Facebook, Instagram e TikTok, são elementos centrais na arquitetura da vigilância, funcionando como intermediárias inevitáveis na vida cotidiana. A ubiquidade dos dispositivos móveis amplia essa dinâmica, possibilitando a coleta de dados sobre localização, hábitos e preferências em tempo real (Castells, 2013).

Essas arquiteturas são desenhadas para promover a permanência e o engajamento dos usuários, maximizando a produção de dados comportamentais excedentes, conforme aponta Zuboff (2019).

O design persuasivo, ou "captology", explora vieses cognitivos para induzir comportamentos desejados, promovendo a maximização do tempo de engajamento e a coleta contínua de dados (Zuboff, 2019). Assim, consolida-se a chamada "economia da atenção", em que o tempo e a concentração do usuário são mercadorias disputadas entre as plataformas (Han, 2018).

No Brasil, o impacto dessa dinâmica é visível na popularização de aplicativos como WhatsApp e TikTok, cuja arquitetura algorítmica orienta o comportamento dos usuários e estrutura práticas sociais cotidianas (Zuboff, 2019; Datafolha, 2023).

O CAPITALISMO DE VIGILÂNCIA NA REALIDADE BRASILEIRA

Embora o Brasil possua mais de 150 milhões de usuários de internet, o acesso é profundamente desigual, refletindo as clivagens sociais e econômicas do país (Cetic.br, 2023). Essa desigualdade cria uma divisão digital que não apenas exclui milhões do acesso à informação, mas também concentra os efeitos mais nocivos do capitalismo de vigilância nas populações vulneráveis, sujeitas a práticas predatórias de coleta de dados.

Embora a penetração da internet tenha aumentado no Brasil, o país ainda convive com um "fosso digital" significativo, especialmente nas regiões Norte e Nordeste. Segundo o Cetic.br (2023), cerca de 20% da população não possui acesso regular à internet, o que compromete o exercício pleno da cidadania digital e evidencia que as formas de vigilância e de coleta de dados atingem desigualmente os grupos sociais.

Esse contexto é agravado pela prática conhecida como "zero rating", em que operadoras oferecem acesso gratuito a determinadas plataformas, como Facebook e WhatsApp, em detrimento do acesso pleno à internet. Isso cria uma internet "empacotada" que limita a diversidade informacional e reforça a dependência das plataformas, principal vetor do capitalismo de vigilância (Zuboff, 2019).

A onipresença de plataformas digitais no Brasil cria um cenário em que o cotidiano da maioria dos cidadãos é mediado por tecnologias de vigilância. Pesquisa do Datafolha (2023) aponta que mais de 95% dos brasileiros que utilizam internet são usuários ativos de WhatsApp, enquanto o Instagram se consolidou como fonte primária de informação para 45% da população.

Esse protagonismo digital, muitas vezes não regulado, expõe milhões de brasileiros a mecanismos opacos de coleta de dados e manipulação comportamental, conforme analisa Zuboff (2019), ampliando o risco de controle social silencioso e efetivo.

As plataformas digitais desempenham um papel central na organização da vida social e econômica no Brasil, desde o comércio eletrônico até as relações interpessoais. O WhatsApp, por exemplo, é a principal ferramenta de comunicação no país, sendo também um vetor fundamental na disseminação de desinformação e na instrumentalização política das redes (Tarrow, 2021).

Essa centralidade reforça a dependência das plataformas e a exposição da população brasileira às dinâmicas do capitalismo de vigilância.

O uso de tecnologias de vigilância pelo Estado brasileiro merece destaque. Diversos programas de segurança pública implementaram sistemas de reconhecimento facial, muitas vezes sem o devido debate público e sem garantias robustas de proteção de dados (Dados.org, 2022).

Outro exemplo é o CadÚnico, banco de dados que reúne informações sensíveis de milhões de brasileiros para a implementação de políticas sociais (Brasil, MDS, 2023). Embora fundamental para a política pública, sua centralização e digitalização suscitam preocupações sobre segurança, privacidade e uso indevido de dados (Dados.org, 2023).

Na saúde, a pandemia de Covid-19 acelerou a digitalização de serviços e a criação de aplicativos como o Conecte SUS, expondo a população a novos riscos relacionados à vigilância sanitária e à segurança da informação (Brasil, 2021).

O uso de reconhecimento facial para fins de segurança pública tem se expandido no Brasil, com casos polêmicos. Destaca-se a atuação do Tribunal de Justiça da Bahia, que, no Processo nº 0005649-90.2020.8.05.0001, confirmou a legalidade do uso de câmeras inteligentes pela Polícia Militar, defendendo o interesse público na segurança. Contudo, organizações de direitos humanos criticam a medida, apontando risco de discriminação e erro, principalmente contra a população negra (Brasil, 2020).

Já no âmbito da saúde pública, o Conecte SUS, sistema que armazena dados sensíveis dos cidadãos, foi alvo de debate judicial quando sofreu ataque hacker em 2021. Embora o STF não tenha julgado diretamente o caso, a Recomendação nº 73 do Conselho Nacional de Justiça, de 2020, já orientava órgãos do Judiciário a priorizarem

medidas de proteção de dados no tratamento de informações pessoais durante a pandemia (CNJ, 2020).

O Cadastro Único para Programas Sociais (CadÚnico) concentra dados de mais de 80 milhões de brasileiros, e sua governança suscita preocupações sobre consentimento e segurança. Em Ação Direta de Inconstitucionalidade (ADI) nº 6.387, o STF discutiu aspectos da Medida Provisória nº 954, de 2020, que determinava o compartilhamento compulsório de dados por empresas de telecomunicação com o IBGE. O Supremo, em decisão histórica, considerou a medida inconstitucional, afirmando que "o direito à proteção de dados pessoais possui estatura constitucional" (Brasil, STF, ADI 6.387, Rel. Min. Rosa Weber, 2020).

Essa decisão fixou um marco relevante ao reconhecer, de forma expressa, a proteção de dados pessoais como direito fundamental, alinhando o Brasil às tendências internacionais.

As populações mais vulneráveis são também as mais afetadas pelo capitalismo de vigilância no Brasil. A utilização de sistemas automatizados para definir acesso a benefícios, serviços ou para fins de segurança pública pode reproduzir e aprofundar discriminações estruturais, um fenômeno conhecido como "racismo algorítmico" (Noble, 2018).

A LGPD E OS LIMITES DA REGULAÇÃO BRASILEIRA

A Lei Geral de Proteção de Dados Pessoais (LGPD), sancionada em 2018, representa um avanço significativo na proteção de dados no Brasil. Inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR) europeu, a LGPD estabelece princípios, direitos e deveres relacionados ao tratamento de dados pessoais (Brasil, 2018).

A LGPD (Lei nº 13.709, de 2018) foi aprovada após amplo debate, com inspiração direta no GDPR europeu, e entrou plenamente em vigor em setembro de 2020. Posteriormente, a Emenda Constitucional nº 115, de 2022, inseriu expressamente a proteção de dados pessoais no rol de direitos fundamentais previstos na Constituição, conferindo ainda mais solidez ao arcabouço protetivo brasileiro (Brasil, 2018).

Apesar dos avanços, a LGPD possui lacunas importantes, sobretudo no que tange à sua efetiva aplicação e fiscalização. A ausência de mecanismos técnicos e institucionais robustos limita sua capacidade de conter as práticas mais lesivas do capitalismo de vigilância (Its Rio, 2022).

Além disso, a LGPD permite exceções amplas para o tratamento de dados pelo Estado, especialmente em áreas como segurança pública, sem garantias suficientes de accountability (Doneda, 2020).

Apesar da constitucionalização, subsistem lacunas normativas. A LGPD prevê exceções significativas, sobretudo para o tratamento de dados pelo Poder Público, que podem ser utilizados para fins de segurança pública, defesa nacional e segurança do Estado, sem sujeição integral às mesmas restrições aplicáveis ao setor privado (art. 4º, III, da LGPD). Tal brecha pode legitimar práticas abusivas de vigilância estatal. Além disso, a figura do consentimento, embora central na LGPD, frequentemente é obtida de forma viciada, por meio de contratos de adesão ou de interfaces confusas, o que viola o princípio da autodeterminação informacional (Its Rio, 2022).

Em comparação com o GDPR, a LGPD apresenta fragilidades em termos de enforcement e proteção de dados sensíveis. Enquanto a União Europeia dispõe de uma tradição consolidada de proteção à privacidade, o Brasil ainda carece de cultura institucional e social nesse campo (Canclini, 2005).

O GDPR europeu consagra uma lógica mais protetiva, destacando, por exemplo, o direito à portabilidade dos dados e ao esquecimento, ambos ainda de implementação incerta no Brasil. O Superior Tribunal de Justiça (STJ) já sinalizou abertura para a aplicação do direito ao esquecimento em certas hipóteses, como na REsp 1.335.153/RJ, mas o Supremo Tribunal Federal (STF), no Tema 786, decidiu que o direito ao esquecimento não é compatível com a Constituição brasileira, o que limita a aplicação dessa garantia no país (Brasil, 2021a; Brasil, 2021b; União Europeia, 2016).

A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão responsável por fiscalizar a aplicação da LGPD. Embora sua criação tenha representado um avanço, sua capacidade operacional e autonomia ainda são limitadas, o que compromete a efetividade da regulação (Its Rio, 2022).

Os tribunais brasileiros, por sua vez, começam a se posicionar sobre questões relativas à proteção de dados, mas a jurisprudência ainda é incipiente (Silva, 2022).

A Autoridade Nacional de Proteção de Dados (ANPD) iniciou sua atuação em 2021, com a publicação de importantes normas orientadoras, como o Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado (ANPD, 2021).

Na seara judicial, destaca-se decisão do Tribunal de Justiça de São Paulo (TJSP), que aplicou pela primeira vez sanções com base na LGPD, condenando uma empresa ao pagamento de indenização por vazamento de dados (TJSP, Apelação Cível nº 1006569-13.2021.8.26.0100). A decisão enfatizou a necessidade de proteção efetiva dos dados pessoais como expressão do direito à personalidade (TJSP, 2022).

IMPACTOS SOCIOPOLÍTICOS NO BRASIL

O capitalismo de vigilância impõe desafios profundos à privacidade e à liberdade individual no Brasil. A coleta massiva e opaca de dados pessoais, muitas vezes sem consentimento livre e informado, compromete a autonomia dos sujeitos e a autodeterminação informacional (Zuboff, 2019). No contexto brasileiro, em que a educação digital é precária e há déficit de conscientização sobre direitos relacionados à privacidade, essa situação é ainda mais grave.

A vigilância ubíqua cria um ambiente em que as escolhas individuais são moldadas de forma imperceptível por sistemas algorítmicos que definem o que é visto, consumido e, muitas vezes, decidido, configurando o que Zuboff chama de "modulação comportamental" (Zuboff, 2019).

O reconhecimento da proteção de dados como direito fundamental pelo STF, na ADI 6.387, criou jurisprudência que fortalece o campo de proteção da privacidade e da autonomia no país (Brasil, 2020). Contudo, o desafio permanece: como operacionalizar essa proteção ante a dinâmica avassaladora das plataformas digitais?

A manipulação comportamental alcança contornos especialmente preocupantes no campo político. A atuação de empresas de marketing digital, a propagação de fake news e o uso de microtargeting eleitoral nas eleições brasileiras revelam o poder das plataformas de moldar a opinião pública e influenciar processos democráticos (Tarrow, 2021).

O caso paradigmático é o das eleições presidenciais de 2018, quando o WhatsApp foi amplamente utilizado para disseminar desinformação de maneira automatizada e massiva, impactando diretamente o debate público e o resultado eleitoral (Dados.org, 2022).

As "bolhas informacionais" criadas pelos algoritmos, que personalizam e filtram conteúdos conforme interesses predefinidos, reforçam a polarização política e corroem a esfera pública deliberativa (Sunstein, 2018).

Além do caso das eleições de 2018, o Tribunal Superior Eleitoral (TSE) tem se posicionado firmemente sobre o combate à desinformação. A Resolução nº 23.610 do TSE, de 2019, introduziu medidas para regular a propaganda eleitoral na internet (Brasil, 2019).

O TSE também criou, em parceria com plataformas, o Programa de Enfrentamento à Desinformação, reconhecendo a necessidade de regular a atuação das big techs no processo eleitoral, como forma de mitigar os efeitos deletérios do capitalismo de vigilância na democracia brasileira.

O capitalismo de vigilância no Brasil opera sobre uma sociedade profundamente marcada por desigualdades raciais e socioeconômicas. A aplicação de sistemas automatizados na segurança pública, como o reconhecimento facial, tem revelado vieses

discriminatórios que reforçam práticas de controle sobre populações historicamente marginalizadas, como jovens negros e periféricos (Noble, 2018).

Pesquisas indicam que sistemas de reconhecimento facial apresentam taxas de erro significativamente mais altas em pessoas negras, ampliando o risco de prisões injustas e violações de direitos (Dados.org, 2022). Assim, a tecnologia não apenas reproduz, mas potencializa estruturas de opressão preexistentes.

A ascensão do capitalismo de vigilância reconfigura a esfera pública brasileira, deslocando o espaço do debate político para ambientes privados controlados por corporações estrangeiras (Castells, 2013). O tradicional espaço público, caracterizado pela pluralidade e pela possibilidade de deliberação democrática, dá lugar a ambientes mediados por algoritmos cujo objetivo principal é a maximização do lucro por meio do engajamento contínuo (Zuboff, 2019).

Essa transformação compromete o ideal habermasiano de esfera pública racional e inclusiva, favorecendo a segmentação e a radicalização das opiniões (Habermas, 1984).

COLONIALISMO DIGITAL E SOBERANIA INFORMACIONAL

Zuboff (2019) descreve a apropriação unilateral de dados pessoais pelas grandes corporações de tecnologia como uma forma de "colonialismo digital". Trata-se de um processo pelo qual os dados gerados por indivíduos e instituições em países periféricos são extraídos, processados e monetizados por empresas sediadas em países centrais, sem que os produtores originais participem dos benefícios econômicos dessa extração.

No Brasil, essa lógica se manifesta de maneira clara: as principais plataformas digitais que dominam o mercado nacional – Google, Meta (Facebook, Instagram, WhatsApp) e Amazon – concentram a capacidade de processamento e análise de dados, enquanto o país permanece como mero fornecedor de matéria-prima informacional (Silveira, 2021).

Esse colonialismo digital reforça uma relação de dependência tecnológica, na qual o Brasil se posiciona como consumidor de tecnologias estrangeiras e fornecedor de dados brutos, sem capacidade soberana de desenvolver e controlar suas próprias infraestruturas digitais (Canclini, 2005).

A desigualdade informacional não é apenas econômica, mas também política e epistemológica, pois limita a capacidade nacional de estabelecer parâmetros próprios para a regulação e ao uso de tecnologias, aprofundando a subordinação aos interesses do capital internacional (Zuboff, 2019).

A luta pela soberania digital emerge, assim, como um dos grandes desafios para o Brasil e demais países do Sul Global. Trata-se da capacidade de estabelecer políticas, infraestruturas e marcos regulatórios que garantam o controle nacional sobre os fluxos de dados e a proteção dos direitos fundamentais de seus cidadãos (Its Rio, 2022).

Nesse sentido, propostas como a construção de data centers locais, o fortalecimento de políticas públicas de inovação tecnológica e a regulamentação estrita da atuação de big techs são caminhos essenciais para reverter o quadro de dependência e vulnerabilidade (Silveira, 2021).

A jurisprudência brasileira começa a refletir sobre a necessidade de soberania digital. O Supremo Tribunal Federal, no julgamento da ADI 5527 (caso WhatsApp), reconheceu que as plataformas devem cumprir decisões judiciais brasileiras, sob pena de violar a soberania nacional (Brasil, 2020).

Embora o STF não tenha decidido pela constitucionalidade do bloqueio judicial do WhatsApp, o julgamento destacou a tensão entre soberania informacional e poder das big techs, apontando para o desafio de estabelecer um marco de regulação efetiva no país (Brasil, 2020).

PERSPECTIVAS DE RESISTÊNCIA E GOVERNANÇA DEMOCRÁTICA

O fortalecimento de marcos regulatórios que restrinjam as práticas predatórias do capitalismo de vigilância é uma das principais estratégias de resistência. A LGPD representa um primeiro passo, mas é necessário avançar em sua aplicação e complementá-la com legislações específicas que regulem a atuação das plataformas digitais, como a recente discussão sobre o Projeto de Lei das Fake News (PL 2.630, de 2020), que busca estabelecer responsabilidades para provedores de redes sociais no Brasil (Brasil, 2020).

Além disso, é imprescindível assegurar a proteção dos dados sensíveis coletados em políticas públicas e ampliar as salvaguardas legais contra o uso discriminatório de tecnologias de vigilância (Dados.org, 2022).

Tramita no Congresso Nacional o Projeto de Lei nº 2.630, de 2020 (PL das Fake News), que busca criar um marco legal para responsabilizar plataformas por conteúdos falsos e combater práticas de manipulação informacional (Brasil, 2020).

Além disso, projetos como o Marco Civil da Inteligência Artificial (PL 21, de 2020) pretendem regulamentar sistemas algorítmicos, visando garantir transparência e accountability (Brasil, 2020).

Diversos teóricos e movimentos sociais têm defendido a concepção de dados como bem comum, ou seja, como recursos coletivos que devem ser geridos

democraticamente e utilizados em prol do interesse público, e não como propriedade privada de corporações (Velkova, 2016).

Essa perspectiva exige uma revisão radical dos fundamentos jurídicos que atualmente permitem a apropriação privatista de dados pessoais, promovendo modelos de governança baseados na participação cidadã e na transparência (Doneda, 2021).

A transparência sobre os algoritmos é tema recorrente na jurisprudência. Em 2022, o Superior Tribunal de Justiça (STJ), no REsp 1.770.105/SP, entendeu que plataformas não são obrigadas a revelar os critérios internos de ranqueamento de conteúdos, sob o argumento de proteção ao segredo empresarial (Brasil, STJ, 2022).

Tal entendimento, entretanto, é criticado por especialistas que defendem que, quando direitos fundamentais estão em jogo, o interesse público deve prevalecer sobre interesses comerciais (Pasquale, 2015).

Outro eixo fundamental da resistência é a promoção da transparência algorítmica, ou seja, a obrigação de que empresas e governos revelem os critérios, processos e impactos de seus sistemas automatizados de decisão (Pasquale, 2015).

A accountability algorítmica envolve não apenas a divulgação dos parâmetros técnicos, mas também a possibilidade efetiva de revisão e de contestação das decisões tomadas por esses sistemas, especialmente quando afetam direitos fundamentais, como no caso de benefícios sociais ou processos criminais (Miranda; Almeida, 2023).

A resistência ao capitalismo de vigilância também se manifesta em ações judiciais protagonizadas por organizações da sociedade civil. O Instituto Brasileiro de Defesa do Consumidor (IDEC) ajuizou diversas ações civis públicas contra empresas por práticas abusivas de coleta e uso de dados, como no caso da ação contra a Serasa Experian, que comercializava dados pessoais sem consentimento, vide a ACP nº 1010290-39.2021.8.26.0100 (IDEC, 2021; TJSP, 2021).

No Brasil, diversas organizações da sociedade civil atuam na resistência ao capitalismo de vigilância, promovendo pesquisas, campanhas e ações jurídicas para defender os direitos digitais. Grupos como o Instituto de Tecnologia e Sociedade do Rio (Its Rio), Coding Rights, Intervozes e Dados.org desempenham papel crucial na denúncia de abusos e na proposição de alternativas democráticas para a governança da internet (Its Rio, 2023; Coding Rights, 2023; Intervozes, 2023; Dados.ORG, 2023).

Esses movimentos se articulam com redes internacionais de resistência digital, evidenciando que a luta contra o capitalismo de vigilância é necessariamente transnacional (Zuboff, 2019).

CONCLUSÃO

Este artigo analisou criticamente o conceito de capitalismo de vigilância, conforme desenvolvido por Shoshana Zuboff, articulando-o com a realidade brasileira. Demonstrou-se que, embora esse fenômeno seja global, sua manifestação no Brasil assume especificidades decorrentes das profundas desigualdades sociais, da fragilidade regulatória e da dependência tecnológica.

Identificou-se que o capitalismo de vigilância impacta diretamente direitos fundamentais – como a privacidade e a liberdade –, reconfigura a esfera pública e aprofunda processos históricos de exclusão e discriminação. Além disso, argumentou-se que a apropriação dos dados brasileiros por grandes corporações estrangeiras constitui uma nova forma de colonialismo digital, que compromete a soberania nacional.

Conclui-se que a resistência a esse modelo exige ações coordenadas em múltiplos níveis: fortalecimento e aprimoramento das regulações nacionais, promoção de alternativas baseadas no interesse público, desenvolvimento de tecnologias autônomas e mobilização social para a defesa dos direitos digitais.

Teve como objetivo central analisar criticamente o fenômeno do capitalismo de vigilância, a partir da perspectiva teórica de Shoshana Zuboff (2019), articulando-o com a realidade brasileira, marcada por profundas desigualdades sociais, fragilidade institucional e dependência tecnológica. O problema que orientou a investigação foi compreender de que modo as práticas de coleta massiva e opaca de dados – típicas do capitalismo de vigilância – impactam os direitos fundamentais no Brasil, especialmente a privacidade, a liberdade e a autodeterminação informacional.

A metodologia adotada foi teórico-conceitual e exploratória, com revisão bibliográfica das principais obras sobre o tema e análise de jurisprudência nacional pertinente, permitindo identificar como o Poder Judiciário brasileiro tem enfrentado os desafios impostos por esse modelo econômico e tecnológico.

Do ponto de vista jurisprudencial, observou-se que o Brasil vem consolidando um importante arcabouço normativo e decisório para a proteção de dados. A decisão do Supremo Tribunal Federal na ADI 6.387 foi paradigmática ao reconhecer, de maneira expressa, a proteção de dados pessoais como direito fundamental, conferindo estatura constitucional ao tema. Esse entendimento foi recentemente reforçado com a Emenda Constitucional nº 115, de 2022, demonstrando um alinhamento progressivo entre a jurisprudência e as tendências internacionais.

Além disso, decisões como o julgamento da ADI 5527, sobre bloqueio do WhatsApp, revelam a preocupação do STF com a defesa da soberania informacional nacional ante a atuação das grandes plataformas. No âmbito infraconstitucional, decisões como a do TJSP (Apelação Cível nº 1006569-13.2021.8.26.0100) mostram que os tribunais locais começam a aplicar efetivamente os dispositivos da Lei Geral de

Proteção de Dados (LGPD), responsabilizando empresas pelo mau uso de informações pessoais.

Contudo, apesar desses avanços, a pesquisa revelou que ainda existem lacunas normativas e institucionais, que dificultam a plena proteção dos cidadãos perante as práticas predatórias do capitalismo de vigilância. A LGPD, embora represente um marco regulatório relevante, apresenta exceções preocupantes, especialmente no tratamento de dados pelo Poder Público, as quais podem legitimar práticas abusivas de vigilância estatal.

Ademais, o colonialismo digital – manifestado na apropriação de dados brasileiros por grandes corporações estrangeiras – reforça a necessidade de políticas públicas voltadas à promoção da soberania digital, como o fortalecimento de infraestruturas tecnológicas nacionais e o desenvolvimento de marcos regulatórios mais robustos, como os que estão sendo debatidos no PL das Fake News e no Marco Legal da Inteligência Artificial.

Por fim, destaca-se que a resistência ao capitalismo de vigilância no Brasil se expressa não apenas no âmbito jurídico, mas também na atuação de movimentos sociais, organizações da sociedade civil e iniciativas acadêmicas que buscam construir uma governança democrática das tecnologias digitais.

Conclui-se que, para enfrentar os desafios postos pelo capitalismo de vigilância, o Brasil precisa consolidar sua cultura institucional de proteção de dados, fortalecer o papel da Autoridade Nacional de Proteção de Dados (ANPD), ampliar a *accountability* algorítmica e fomentar a transparência das práticas empresariais e estatais de coleta e tratamento de dados. Apenas assim será possível garantir que o país avance na construção de uma sociedade digital que respeite e promova os direitos fundamentais, reafirmando a centralidade da liberdade e da dignidade humanas ante as novas formas de poder informacional.

No horizonte, permanece a necessidade de uma reflexão crítica sobre as formas de liberdade e de autonomia na era digital, reconhecendo que a construção de uma sociedade mais justa e democrática passa, necessariamente, pelo enfrentamento dos desafios colocados pelo capitalismo de vigilância.

Este artigo demonstrou que, no Brasil, o capitalismo de vigilância atua sobre um terreno marcado por desigualdades históricas e institucionais, mas que também é palco de resistências significativas, tanto institucionais quanto sociais.

A jurisprudência brasileira evolui para reconhecer e proteger direitos fundamentais relacionados à privacidade e à proteção de dados, mas enfrenta desafios diante da assimetria de poder entre Estado, cidadãos e corporações transnacionais.

O enfrentamento do capitalismo de vigilância exige o fortalecimento das instituições reguladoras, a consolidação de uma cultura jurídica voltada à proteção de dados e o fomento a alternativas democráticas e inclusivas de governança digital.

REFERÊNCIAS

BRASIL. Autoridade Nacional de Proteção de Dados. **Guia orientativo para definição dos agentes de tratamento de dados pessoais e do encarregado.** Brasília, DF: ANPD, 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-agentes-de-tratamento.pdf. Acesso em: 2 jun. 2025.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: Senado Federal, 1988.

BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**: Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Brasília, DF, 15 ago. 2018.

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.

BRASIL. Congresso Nacional. Senado Federal. **Projeto de Lei n.º 2.630, de 2020**. Estabelece a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet, altera a Lei nº 12.965/2014 (Marco Civil da Internet). Brasília, DF, 2020. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/141944. Acesso em: 2 jun. 2025.

BRASIL. Congresso Nacional. Câmara dos Deputados. **Projeto de Lei n.º 21, de 2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil. Brasília, DF, 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2239760. Acesso em: 2 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 6.387**. Relatora: Min. Rosa Weber. Brasília, DF, 2020. Disponível em: https://www.stf.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Ação Direta de Inconstitucionalidade nº 5.527**. Relator: Min. Edson Fachin. Brasília, DF, 2021. Disponível em: https://www.stf.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Supremo Tribunal Federal. **Recurso Extraordinário com Repercussão Geral n. 1.010.606/RJ (Tema 786)**. Relator: Min. Dias Toffoli. Brasília, DF, 2021. Disponível em: https://www.stf.jus.br. Acesso em: 2 jun. 2025.

BRASIL. **Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome (MDS).** Cadastro Único para Programas Sociais. Brasília: MDS, 2023. Disponível em: https://www.gov.br/mds/pt-br/acoes-e-programas/cadastro-unico. Acesso em: 2 jun. 2025.

BRASIL. Ministério da Saúde. **Conecte SUS: saiba como funciona. Brasília: Ministério da Saúde, 2021.** Disponível em: https://www.gov.br/saude/conectesus. Acesso em: 2 jun. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial n. 1.335.153 - RJ (2012/0185646-6). Relator: Min. Luis Felipe Salomão.** Brasília, DF, 15 out. 2013. Disponível em: https://www.stj.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1.770.105/SP. Relator: Ministro Paulo de Tarso Sanseverino**. Brasília, julgado em 28 set. 2022. Disponível em: https://www.stj.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Tribunal de Justiça da Bahia. **Decisão do Processo nº 0005649-90.2020.8.05.0001 confirma legalidade de câmeras com reconhecimento facial.** Salvador: TJBA, 2020. Disponível em: https://www.tjba.jus.br. Acesso em: 2 jun. 2025.

BRASIL. Tribunal Superior Eleitoral. **Resolução nº 23.610, de 18 de dezembro de 2019**. Estabelece normas para a propaganda eleitoral, utilização e geração do horário gratuito e condutas ilícitas em campanha eleitoral. Diário da Justiça Eletrônico, Brasília, DF, 20 dez. 2019. Disponível em: https://www.tse.jus.br/legislacao/compilada/res/2019/resolucao-no-23-610-de-18-de-dezembro-de-2019. Acesso em: 2 jun. 2025.

CANCLINI, Néstor García. **Consumidores e cidadãos: conflitos multiculturais da globalização**. 5. ed. Rio de Janeiro: UFRJ, 2005.

CASTELLS, Manuel. **A galáxia da internet: reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2013.

CETIC.br. **TIC Domicílios 2023: Pesquisa sobre o uso das Tecnologias de Informação e Comunicação nos domicílios brasileiros**. São Paulo: Comitê Gestor da Internet no Brasil, 2024.

CONSELHO NACIONAL DE JUSTIÇA (Brasil). Recomendação nº 73, de 20 de agosto de 2020. **Recomenda aos órgãos do Poder Judiciário a observância de medidas voltadas à proteção de dados pessoais no uso de tecnologias no contexto da pandemia da Covid-19.** Brasília: CNJ, 2020. Disponível em: https://atos.cnj.jus.br/atos/detalhar/3395. Acesso em: 2 jun. 2025.

CODING RIGHTS. Disponível em: https://codingrights.org. Acesso em: 2 jun. 2025.

DADOS.org. **Relatório sobre tecnologias de vigilância no Brasil**. São Paulo: DADOS.org, 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Forense, 2020.

DELEUZE, Gilles. **Post-scriptum sobre as sociedades de controle**. In: DELEUZE, Gilles. Conversações. São Paulo: Editora 34, 1992. p. 219-226.

HABERMAS, Jürgen. **Mudança Estrutural da Esfera Pública**. Rio de Janeiro: Tempo Brasileiro, 1984.

HAN, Byung-Chul. **Sociedade do cansaço**. Petrópolis: Vozes, 2018.

IDEC – INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **Ações civis públicas para proteção de dados pessoais**. São Paulo, 2021. Disponível em: https://idec.org.br. Acesso em: 2 jun. 2025.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA (IBGE). **Pesquisa Nacional por Amostra de Domicílios Contínua: acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal**. Rio de Janeiro: IBGE, 2022.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO (ITS Rio). **Guia da LGPD para cidadãos.** Rio de Janeiro: ITS Rio, 2022.

INTERVOZES. Disponível em: https://intervozes.org.br. Acesso em: 2 jun. 2025.

MIRANDA, Carla; ALMEIDA, João. **Accountability e sistemas algorítmicos: desafios para a proteção de direitos fundamentais.** São Paulo: Editora Jurídica, 2023.

NOBLE, Safiya Umoja. **Algorithms of oppression: how search engines reinforce racism**. New York: NYU Press, 2018.

PASQUALE, Frank. **The black box society: the secret algorithms that control money and information.** Cambridge: Harvard University Press, 2015.

SÃO PAULO (Estado). Tribunal de Justiça. **Apelação Cível nº 1006569-13.2021.8.26.0100,** 12ª Câmara de Direito Privado, Rel. Des. José Carlos Ferreira Alves, julgado em 29 mar. 2022, publicado em 1º abr. 2022. Disponível em: https://esaj.tjsp.jus.br. Acesso em: 2 jun. 2025.

SILVA, Mariana de Almeida. **A proteção de dados pessoais no Brasil: avanços e desafios da jurisprudência**. São Paulo: Revista dos Tribunais, 2022.

SILVEIRA, Sérgio Amadeu da. **Exclusão digital: a miséria na era da informação**. São Paulo: Fundação Perseu Abramo, 2021.

SILVEIRA, Sérgio Amadeu da. **Tecnopolítica e o enfraquecimento da democracia**. São Paulo: Fundação Perseu Abramo, 2021.

SUNSTEIN, Cass R. **Republic: divided democracy in the age of social media**. Princeton: Princeton University Press, 2018.

TARROW, Sidney. **O poder em movimento: os movimentos sociais e o conflito político**. Petrópolis: Vozes, 2021.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. **Apelação Cível nº 1010290-39.2021.8.26.0100.** São Paulo, 2021. Disponível em: https://www.tjsp.jus.br. Acesso em: 2 jun. 2025.

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 (Regulamento Geral sobre a Proteção de Dados – GDPR). Jornal Oficial da União Europeia, L119, p. 1–88, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 2 jun. 2025.

VELKOVA, Julia. **Data as commons**. In: SCHÄFER, Mirko Tobias; VAN ES, Karin (org.). The datafied society: studying culture through data. Amsterdam: Amsterdam University Press, 2016. p. 87-104.

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

Recebido em: 03/06/25
Aprovado em: 25/08/25