

FORUM SHOPPING, BIG TECHS E SOBERANIA DIGITAL: ASSIMETRIA REGULATÓRIA, FRAGMENTAÇÃO NORMATIVA E OS DESAFIOS AO BRASIL

FORUM SHOPPING, BIG TECHS AND DIGITAL SOVEREIGNTY: REGULATORY ASYMMETRY, NORMATIVE FRAGMENTATION AND THE CHALLENGES TO BRAZIL

FORUM SHOPPING, GRANDES TECNOLÓGICAS Y SOBERANÍA DIGITAL: ASIMETRÍA REGULATORIA, FRAGMENTACIÓN NORMATIVA Y LOS DESAFÍOS A BRASIL

Eduardo Augusto Nascimento Souza¹

João Vitor Paixão Lopes²

Lucas Silva Souza³

Rafael Freire Ferreira⁴

RESUMO: Este artigo examinou a prática de *forum shopping* regulatório por Big Techs como estratégia para eludir a proteção de dados pessoais e a soberania digital brasileira. Investiga-se em que medida essa arbitragem entre jurisdições compromete a eficácia da Lei Geral de Proteção de Dados Pessoais (LGPD), notadamente fiscalização, sanções e tutela dos titulares. A hipótese é a de que o *forum shopping* regulatório — categoria distinta do *forum shopping* judicial — compromete parcialmente essas dimensões mediante três mecanismos (fragmentação societária, eleição de foro estrangeiro e dispersão geográfica da infraestrutura de dados), mitigáveis pelo fortalecimento da ANPD, por alianças regulatórias internacionais e pela capacidade tecnológica autônoma. A pesquisa, qualitativa, bibliográfica e documental, comparou GDPR, CCPA e LGPD. Os resultados demonstraram que a assimetria entre esses marcos cria incentivos estruturais à arbitragem regulatória e que o Brasil avançou no plano normativo, embora sua eficácia seja limitada pela captura regulatória informacional, pela dependência infraestrutural e pela assimetria de recursos entre regulador e regulado. Concluiu-se que o *forum shopping* persiste como fenômeno estrutural, exigindo medidas coordenadas nas três frentes propostas.

Palavras-chave: Proteção de dados. Big Techs. *Forum shopping*. Soberania digital. Assimetria regulatória.

¹ Graduando em Direito pela Faculdade de Excelência UNEX de Itabuna (UNEX) — IMES. Especialista em Direito Tributário e Contabilidade (FACUMINAS, 2026); Especialista em Direito Digital (FACUMINAS, 2025); Especialista em Direito da Criança, do Adolescente e do Idoso (FACUMINAS, 2025); Especialista em Direito Trabalhista (UNIASSELVI, 2024); Especialista em Direito Penal (UNIASSELVI, 2023); Especialista em Direito Trabalhista Penal (FACUMINAS, 2023); Especialista em Investigação Forense e Perícia Criminal (UNIASSELVI, 2023); Licenciado em Filosofia pela Universidade Estadual de Santa Cruz (UESC, 2006); Técnico Administrativo Ministerial no Ministério Público da Bahia (MP/BA).

² Graduando em Direito pela Faculdade de Excelência UNEX de Itabuna (UNEX) — IMES.

³ Graduando em Direito pela Faculdade de Excelência UNEX de Itabuna (UNEX) — IMES. Graduado em Engenharia Ambiental pela FTC/UNEX (2012).

⁴ Professor do Curso de Direito da Faculdade de Excelência UNEX de Itabuna (UNEX) — IMES. Bacharel em Direito (FTC); Bacharel em Administração (UESC); Especialista em Direito Público (UGF); Especialista em Ciências de Dados e Big Data Analytics (FAMEESP); Pós-Graduando em Educação Superior (Anhanguera); Mestre em Direito (Universidade Autónoma de Lisboa); Doutorando em Direito (Universidad de Salamanca); Graduando em Licenciatura em História (Fatecie).

ABSTRACT: This article examined the practice of regulatory *forum shopping* by Big Techs as a strategy to circumvent personal data protection and Brazilian digital sovereignty. It investigates to what extent this jurisdiction arbitrage compromises the effectiveness of the Brazilian General Data Protection Law (LGPD), notably oversight, sanctions and the protection of data subjects' rights. The hypothesis holds that regulatory *forum shopping* — a category distinct from judicial *forum shopping* — partially compromises these dimensions through three mechanisms (corporate fragmentation, foreign forum selection and geographic dispersion of data infrastructure), mitigable by strengthening the National Data Protection Authority (ANPD), international regulatory alliances and autonomous technological capacity. The research, qualitative, bibliographic and documentary, compared the GDPR, the CCPA and the LGPD. The results showed that the asymmetry between these frameworks creates structural incentives for regulatory arbitrage and that Brazil has advanced in the normative sphere, although its effectiveness is limited by informational regulatory capture, infrastructural dependence and the asymmetry of resources between regulator and regulated. It was concluded that *forum shopping* persists as a structural phenomenon, requiring coordinated measures on the three proposed fronts.

Keywords: Data protection. Big Techs. *Forum shopping*. Digital sovereignty. Regulatory asymmetry.

RESUMEN: Este artículo examinó la práctica de *forum shopping* regulatorio por grandes tecnológicas como estrategia para eludir la protección de datos personales y la soberanía digital brasileña. Se investiga en qué medida este arbitraje entre jurisdicciones compromete la eficacia de la Ley General de Protección de Datos Personales (LGPD), especialmente fiscalización, sanciones y tutela de los derechos de los titulares. La hipótesis es que el *forum shopping* regulatorio — categoría distinta del *forum shopping* judicial — compromete parcialmente esas dimensiones mediante tres mecanismos (fragmentación societaria, elección de foro extranjero y dispersión geográfica de la infraestructura de datos), mitigables mediante el fortalecimiento de la Autoridad Nacional de Protección de Datos (ANPD), alianzas regulatorias internacionales y capacidad tecnológica autónoma. La investigación, cualitativa, bibliográfica y documental, comparó el GDPR, la CCPA y la LGPD. Los resultados demostraron que la asimetría entre estos marcos crea incentivos estructurales al arbitraje regulatorio y que Brasil avanzó en el plano normativo, aunque su eficacia está limitada por la captura regulatoria informacional, la dependencia infraestructural y la asimetría de recursos entre regulador y regulado. Se concluyó que el *forum shopping* persiste como fenómeno estructural, exigiendo medidas coordinadas en los tres frentes propuestos.

Palabras clave: Protección de datos. Grandes tecnológicas. *Forum shopping*. Soberanía digital. Asimetría regulatoria.

1. INTRODUÇÃO

Na economia digital, os dados pessoais constituem o recurso mais valioso — e, paradoxalmente, o mais vulnerável. Algoritmos processam silenciosamente cada fragmento de informação, transformando escolhas cotidianas em insumos para mercados preditivos (Zuboff, 2019). Nesse cenário, as grandes corporações de tecnologia — Google, Meta, Amazon, Apple e Microsoft — deixaram de ser meras prestadoras de serviços para se tornar atores transnacionais cujo poder frequentemente desafia a capacidade regulatória dos Estados (Cohen, 2019).

Uma das estratégias mais reveladoras desse fenômeno é o chamado *forum shopping* regulatório: a prática, adotada por essas empresas, de selecionar jurisdições que lhes sejam mais

favoráveis — seja para sediar operações, firmar contratos ou fragmentar a infraestrutura de dados — com o objetivo de escapar, total ou parcialmente, da incidência de normas protetivas mais rigorosas. A distinção entre essa categoria e o *forum shopping* judicial, bem como seus desdobramentos sobre a escolha de lei aplicável, será examinada em detalhe na seção 3.2.

A questão que orienta este trabalho é, portanto, a seguinte: em que medida o *forum shopping* regulatório praticado por Big Techs compromete a eficácia da Lei Geral de Proteção de Dados Pessoais (LGPD) e a afirmação da soberania digital brasileira?

A relevância de investigar esse problema decorre da confluência de três fatores interligados. O primeiro é a heterogeneidade do cenário global de proteção de dados: o GDPR (*General Data Protection Regulation*), a CCPA (*California Consumer Privacy Act*) e a LGPD criam um mosaico normativo que incentiva a arbitragem regulatória pelas grandes plataformas (Mendes, 2019). O segundo é a dependência estrutural do Brasil em relação à infraestrutura digital estrangeira (Floridi, 2020). O terceiro são os recentes movimentos institucionais brasileiros — a virada jurisprudencial do STF (Supremo Tribunal Federal) no RE (Recurso Extraordinário) 1.037.396 (Tema 987), os Decretos nº 12.975 e 12.976/2026 e o Estatuto da Criança e do Adolescente Digital (Lei 15.211/2025) — que impõem uma reavaliação crítica do panorama regulatório.

O objetivo geral deste artigo é examinar como o *forum shopping* das Big Techs opera como mecanismo de elusão da proteção de dados e em que termos desafia a soberania digital brasileira. Três objetivos específicos orientam a investigação: analisar a disparidade entre os marcos do GDPR, da CCPA e da LGPD, compreendendo como essa heterogeneidade viabiliza o *forum shopping* como consequência estrutural do desenho institucional vigente; identificar as práticas corporativas de exploração de jurisdições favoráveis; e avaliar as respostas institucionais brasileiras — seus avanços e limites — diante desse quadro.

A hipótese é a de que o *forum shopping* regulatório compromete parcialmente a eficácia da LGPD e a soberania digital brasileira, mas que seus efeitos podem ser mitigados em três frentes: o fortalecimento institucional da ANPD (Autoridade Nacional de Proteção de Dados), com atuação proativa e tecnicamente capacitada; a construção de alianças regulatórias internacionais, para ampliar a pressão do Brasil e reduzir a arbitragem regulatória; e o desenvolvimento progressivo de capacidade tecnológica autônoma, que reduza a dependência externa.

2. MÉTODOS

O presente artigo foi desenvolvido a partir de pesquisa qualitativa, bibliográfica e documental, adotando-se a análise comparativa entre marcos regulatórios como procedimento central. A opção pela abordagem qualitativa justifica-se pela natureza do objeto: examinar práticas de *forum shopping* por Big Techs demanda compreensão aprofundada de fenômenos jurídicos, econômicos e institucionais não suscetíveis de quantificação direta.

As fontes de dados compreenderam três categorias, selecionadas segundo critérios de pertinência temática, atualidade e relevância institucional. A primeira é a legislação nacional e estrangeira: Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), Marco Civil da Internet (Lei nº 12.965/2014), Código de Defesa do Consumidor (Lei nº 8.078/1990), Código de Processo Civil (Lei nº 13.105/2015), Estatuto da Criança e do Adolescente Digital (Lei nº 15.211/2025), Decretos nº 12.975 e 12.976/2026, Emenda Constitucional nº 115/2022, GDPR e *California Consumer Privacy Act* (CCPA). A segunda é a jurisprudência, selecionada por sua pertinência direta à proteção de dados e à regulação de plataformas: a ADI (Ação Direta de Inconstitucionalidade) 6.387 (constitucionalidade da LGPD e reconhecimento da proteção de dados como direito fundamental), o RE 1.037.396, Tema 987 (reinterpretação do art. 19 do Marco Civil) e, complementarmente, a ADPF (Arguição de Descumprimento de Preceito Fundamental) 572 e as ADIs 5.527 e 7.261 (liberdade de expressão e moderação de conteúdo). A terceira é a doutrina nacional e internacional, abrangendo autores que investigam o capitalismo de vigilância, a governamentalidade algorítmica, a proteção de dados, o direito internacional privado e a soberania digital.

O procedimento analítico foi estruturado em três etapas. Na primeira, realizou-se a revisão de literatura por fichamentos estruturados, extraíndo conceitos, teses e citações pertinentes a cada eixo temático. Na segunda, procedeu-se à análise comparativa dos marcos regulatórios, empregando categorias analíticas homogêneas — natureza jurídica da proteção de dados, âmbito de aplicação territorial, bases legais de tratamento, direitos dos titulares, sanções e mecanismos de *enforcement* — para identificar convergências e divergências entre os modelos europeu, norte-americano e brasileiro. Na terceira, os achados foram submetidos à análise crítica para avaliar a eficácia das respostas institucionais brasileiras diante do fenômeno do *forum shopping*.

O recorte temporal adotado abrange o período de 2006 a 2026, tomando como marco inicial a obra de Doneda sobre a evolução da privacidade à proteção de dados, e como marco final as reformas regulatórias brasileiras de 2025-2026. As bases bibliográficas consultadas compreenderam periódicos científicos, obras doutrinárias e documentos normativos oficiais, nacionais e estrangeiros. A escolha do recorte justifica-se por contemplar tanto a consolidação teórica do campo quanto as transformações normativas mais recentes.

Entre as limitações metodológicas, destaca-se a impossibilidade de acesso a dados empíricos sobre a frequência e a magnitude do *forum shopping* praticado por Big Techs no Brasil, uma vez que tais informações, quando existentes, são mantidas sob sigilo empresarial ou classificadas como segredo de justiça em litígios em curso. Ademais, as reformas de 2025-2026 são recentes, não havendo ainda jurisprudência consolidada sobre sua aplicação, o que impõe cautela na generalização dos achados. Registra-se, ainda, que a análise distingue a possibilidade teórica de arbitragem regulatória da comprovação empírica de sua efetiva utilização por empresas específicas.

Quanto ao uso de ferramentas de inteligência artificial, cumpre registrar que o presente artigo foi elaborado com o auxílio de assistente de IA (modelo de linguagem natural) utilizado exclusivamente como ferramenta de apoio à revisão textual, à organização estrutural do conteúdo e à sugestão de formulações, sob integral supervisão e responsabilidade dos autores. Todas as fontes, referenciais teóricos, dados normativos e jurisprudenciais foram previamente selecionados, verificados e validados pelos autores, não tendo a IA gerado conteúdo autônomo ou substituído a análise crítica humana. A redação final, a argumentação, a escolha das fontes e a posição teórica adotada são de responsabilidade exclusiva dos autores.

O estudo não envolveu pesquisa direta com seres humanos ou animais, dispensando-se, portanto, a submissão a comitê de ética em pesquisa, nos termos da Resolução CNS nº 510/2016.

3. RESULTADOS E DISCUSSÕES

3.1 Assimetria Regulatória Global e Incentivos ao Forum Shopping

A sociedade informacional reposicionou os dados pessoais no centro da dinâmica econômica e política contemporânea. Zuboff (2019) denominou *capitalismo de vigilância* o regime no qual a experiência humana é convertida em excedente comportamental e comercializada

como predições — uma mutação em que o produto é o próprio comportamento humano projetado. Esse modelo é viabilizado pelo que Rouvroy e Berns (2015) chamam de *governamentalidade algorítmica*: uma gestão social que opera pela construção de perfis preditivos, dispensando a deliberação racional e a justificação pública do poder estatal. Alves e Andrade (2022) advertem que esse processo reduz a autonomia individual, gerando subjetividades rarefeitas, menos capazes de reflexão crítica.

As Big Techs — Google, Meta, Amazon, Apple e Microsoft — são os principais agentes desse regime. Seu poder transcende o processamento de informações: elas controlam a infraestrutura digital sobre a qual Estados e cidadãos operam, criando uma dependência que compromete a autonomia digital de nações periféricas. Para Couldry e Mejias (2019), isso configura *colonialismo digital* — os dados fluem do Sul global para os servidores das corporações, onde são monetizados, enquanto os benefícios se concentram nos países sede. É nesse contexto que Floridi (2020) define a *soberania digital* como a capacidade de um Estado exercer autodeterminação normativa sobre seu ambiente digital e os dados de seus cidadãos. Trata-se, todavia, de noção multidimensional, que não se esgota no domínio estatal absoluto sobre a infraestrutura tecnológica: abrange igualmente a capacidade de estabelecer regras, fiscalizar agentes econômicos, proteger direitos fundamentais e manter autonomia estratégica em áreas tecnológicas essenciais. Turobov, Carrapico e Farrand (2026) evidenciam, no contexto europeu, que a soberania digital é um conceito funcionalmente diferenciado, cujo conteúdo varia conforme a instituição que o mobiliza; Lim (2026), por sua vez, adverte para os *trade-offs* inerentes às políticas de controle digital, que podem comprometer a abertura e a inovação quando implementadas de modo exclusivamente reativo.

Os ordenamentos jurídicos que disciplinam a proteção de dados não são uniformes, e essa heterogeneidade tem consequências concretas. O GDPR consolidou-se como o paradigma mais rigoroso, não apenas pela severidade das sanções, mas pelo caráter preventivo e exauriente da norma: estabelece limites claros para o tratamento de dados, reduzindo lacunas ao mínimo. Seu modelo assenta-se em cinco pilares — consentimento qualificado; responsabilidade demonstrável (*accountability*); avaliação de impacto; portabilidade; e sanções sobre o faturamento global do infrator (Doneda, 2006; Kuner, 2013). Esse desenho fez do GDPR uma referência global que influenciou legislações ao redor do mundo, inclusive a LGPD.

O próprio desenho do GDPR, todavia, criou uma vulnerabilidade que as Big Techs exploram. O mecanismo do *one-stop shop* (art. 56) estabelece que a autoridade do estabelecimento principal conduz investigações transfronteiriças. As plataformas concentraram suas sedes europeias na Irlanda, país de regulação mais leniente. A *Data Protection Commission* irlandesa, responsável por Google, Meta, Apple, TikTok e Twitter/X, tornou-se o gargalo do sistema, com investigações que se arrastam por anos e sanções reduzidas (Kuner, 2013; Cohen, 2019). Esse "*Irish forum shopping*" revela que o desequilíbrio regulatório opera também no interior do sistema europeu.

Em posição oposta, o modelo norte-americano revela uma contradição estrutural. Os Estados Unidos, arautos da liberdade de mercado, viram-se forçados a reconhecer que o espaço deixado ao arbítrio das corporações não era liberdade, mas ausência de direitos. O escândalo da Cambridge Analytica — que expôs o uso de dados do Facebook para microdirecionamento político nas eleições de 2016 e no Brexit — demonstrou que a proteção de dados é condição para a integridade democrática (Zuboff, 2019; Richards, 2021). A reação, contudo, não produziu uma lei federal: o que se seguiu foi um mosaico de legislações estaduais, cujo principal expoente é a CCPA, ampliada pela CPRA (*California Privacy Rights Act*).

A CCPA caracteriza-se por uma abordagem setorial e mais tímida que a europeia. Assenta-se no direito de *opt-out* em vez do consentimento prévio do GDPR; não cria agência federal dedicada; e suas sanções são mais brandas. Schwartz e Solove (2011) demonstram que a diferença é conceitual: a noção de "informação pessoalmente identificável" (PII) nos EUA é mais restrita que "dado pessoal" no GDPR, excluindo categorias inteiras de dados.

O paradoxo americano não reside na ausência de regulação — a Califórnia tem lei própria —, mas na dispersão institucional e na resistência a tratar a proteção de dados como direito fundamental. O resultado é um ambiente reativo e setorial, que deixa espaços para as Big Techs orientarem suas operações às jurisdições menos exigentes.

O Brasil, com a LGPD (Lei nº 13.709/2018), ocupa posição peculiar no cenário global. A lei filia-se ao modelo europeu: inspira-se no GDPR, adota as mesmas bases legais, assegura direitos análogos aos titulares e institui a ANPD como órgão fiscalizador. No plano constitucional, a EC (Emenda Constitucional) 115/2022 elevou a proteção de dados a direito fundamental autônomo (art. 5º, LXXIX, da CF/88) (Constituição Federal de 1988),

consolidando o que Mendes (2019) descreve como constitucionalização da proteção de dados — movimento que nem os EUA realizaram em âmbito federal.

A LGPD, todavia, revela limitações estruturais que a distanciam do paradigma europeu. A primeira é o teto sancionatório: o GDPR permite multas de até 4% do faturamento global, sem limite absoluto; a LGPD fixa o teto em 2% do faturamento no Brasil, limitado a R\$ 50 milhões — valor significativamente inferior, considerando que o faturamento das Big Techs no país é fração do global (Bioni, 2019).

A segunda limitação é institucional: a ANPD, criada como órgão vinculado à Presidência, apenas recentemente foi fortalecida pelos Decretos nº 12.975 e 12.976/2026, mas sua capacidade operacional ainda é incompatível com a magnitude do desafio (Ferreira, 2020). A terceira é a ausência de *adequacy decision* da UE para o Brasil, fazendo com que o fluxo de dados dependa de cláusulas contratuais padrão, o que eleva a complexidade e os custos de conformidade.

A posição brasileira é híbrida e paradoxal. Formalmente, a LGPD é uma das leis mais avançadas do Sul global. Materialmente, sua eficácia é limitada pelo teto sancionatório reduzido, pela incipiência operacional da ANPD, pela dependência de provedores estrangeiros de nuvem e pela falta de reconhecimento internacional. Essa distância entre o texto legal e a efetividade concreta é o desafio central que Mendes (2019) já identificava: a transição de um modelo formalmente robusto para materialmente eficaz depende de condições ainda não realizadas. É nessa distância que o *forum shopping* encontra seu terreno mais fértil.

Mendes (2019) e Bioni (2019) apontam ainda para a fragmentação normativa global: o mundo não caminha para a harmonização, mas para um mosaico de regimes concorrentes, cada qual com seu âmbito, sanções e exigências — disparidade que, como demonstrado, cria aberturas estratégicas exploradas pelas Big Techs e opera como condição estrutural para o *forum shopping*.

3.2 Forum Shopping em Camadas

A origem do *forum shopping* não é nova: remonta ao direito internacional privado, onde designava a faculdade de o autor escolher, entre jurisdições concorrentes, aquela mais favorável. Gaillard (2010), em sua teoria geral da arbitragem internacional, oferece chave teórica para compreender a dimensão desse fenômeno ao identificar três representações: a monolocal, que vincula a arbitragem a um ordenamento estatal específico; a westfaliana, que reconhece a

concorrência entre ordens jurídicas nacionais; e a autônoma, na qual a arbitragem opera como ordem jurídica independente, desvinculada de qualquer soberania estatal. É essa terceira representação que importa: na ausência de um órgão internacional central que uniformize a arbitragem — um vácuo institucional —, os atores transnacionais ganham liberdade para escolher, entre ordenamentos concorrentes, aquele que melhor lhes atende, fragilizando particularmente as nações com menor capacidade de impor sua jurisdição. A falta de uma autoridade arbitral global opera, portanto, como condição estrutural para a exploração de disparidades regulatórias.

Cumprido, contudo, precisar a categoria analítica adotada. O *forum shopping* judicial, figura clássica do direito internacional privado, refere-se à escolha da jurisdição processual mais favorável entre as concorrentes. No contexto das Big Techs, essa lógica transcende o plano processual e converte-se em estratégia corporativa de arbitragem regulatória, que não se confunde com a mera escolha de lei aplicável: envolve a estruturação deliberada de operações societárias, contratuais e infraestruturais para se situar em jurisdições de ambiente normativo menos exigente. Essa distinção é essencial, pois o fenômeno aqui examinado opera antes mesmo do litígio, na própria arquitetura organizacional das plataformas.

Com a globalização e a ascensão das Big Techs, a lógica do *forum shopping* transcendeu o âmbito processual para se converter em expediente corporativo permanente. As plataformas estruturam suas operações societárias, contratuais e infraestruturais para se situar nas jurisdições de ambiente normativo menos exigente, prática que se viabiliza pela arquitetura societária das grandes plataformas — como ilustra o fenômeno do "Irish forum shopping", examinado na subseção anterior.

Importa, todavia, distinguir, com precisão jurídica, a legítima organização empresarial internacional — que responde a razões econômicas, fiscais e operacionais lícitas — das estruturas eventualmente utilizadas para dificultar a aplicação da legislação. A mera presença de subsidiárias em múltiplas jurisdições não configura, por si só, *forum shopping*; o que caracteriza a arbitragem regulatória é a utilização deliberada dessa dispersão geográfica para elidir a incidência de normas protetivas e fragilizar a responsabilização.

Kuner (2013) já advertia que a fragmentação regulatória e a ausência de coordenação entre autoridades nacionais criam incentivos estruturais para que as corporações explorem as lacunas do sistema, transferindo dados para jurisdições com menor capacidade fiscalizatória. Não se

trata de escolha isolada, mas de estratégia mais ampla de distribuição geográfica da estrutura corporativa: cada subsidiária opera sob a lei local, enquanto o controle efetivo e o processamento estratégico dos dados permanecem centralizados na matriz.

Essa dinâmica encontra amparo em Cohen (2019), para quem o capitalismo informacional opera por meio da indistinção entre os mecanismos de produção de verdade e as estruturas de poder privado — as plataformas não apenas se submetem às normas, mas remodelam a arquitetura institucional que as regula. As regras técnicas e legais que governam os fluxos de informação estão estruturalmente desequilibradas, permitindo que o poder corporativo transnacional se sobreponha à deliberação democrática dos Estados. Richards (2021) oferece chave complementar: a privacidade é questão de poder — a informação confere poder sobre seres humanos, e as regras de proteção de dados existem para contê-lo. O *forum shopping* revela-se, nesse quadro, como a estratégia mediante a qual as Big Techs buscam escapar das contenções que os ordenamentos nacionais tentam impor.

A esse aspecto soma-se a seleção do foro contratual. Os contratos de adesão das plataformas — termos de serviço e políticas de privacidade — frequentemente elegem tribunais estrangeiros e aplicam legislações de baixa proteção. Frazão e Santos (2020) demonstram como as plataformas exercem poder de mercado por meio de cláusulas que restringem a autonomia dos usuários e dificultam a responsabilização — fenômeno que denominam "*data-opolies*", em que o controle sobre dados e o poder contratual se retroalimentam. No Brasil, o CDC (Código de Defesa do Consumidor) (art. 51, IV e XVII) e o CPC (Código de Processo Civil) (arts. 21 e 25) oferecem instrumentos para nulificar tais cláusulas, mas sua aplicação depende de iniciativa do usuário lesado e da capacidade das autoridades de fazer prevalecer a jurisdição nacional — o que, na prática, raramente ocorre em escala. Cumpre, ainda, distinguir as categorias envolvidas: foro contratual (cláusula de eleição de foro), lei aplicável (direito material regente da relação) e jurisdição competente (poder do Estado de julgar) não são equivalentes, e a análise de cada uma exige tratamento próprio, considerando-se os limites impostos pelo ordenamento brasileiro à eficácia dessas cláusulas e a eventual incidência de normas de aplicação extraterritorial.

O *forum shopping* também se manifesta no plano da infraestrutura digital. As Big Techs controlam a camada física da internet — servidores, cabos submarinos, data centers e serviços de nuvem — e fragmentam essa infraestrutura entre jurisdições para dificultar a aplicação de leis locais. Se um dado de usuário brasileiro está armazenado nos Estados Unidos, processado

na Irlanda e acessível por subsidiária em Singapura, a questão sobre qual lei rege sua proteção torna-se consideravelmente complexa. Essa fragmentação é forma de elusão normativa: ao espalhar geograficamente os componentes técnicos, as plataformas criam um emaranhado jurisdicional no qual a responsabilidade se dilui. Pereira e Faleiros Júnior (2024) concluem que a dependência tecnológica limita severamente a eficácia de medidas regulatórias unilaterais, sendo necessária articulação entre política antitruste, direitos humanos e inovação estatal.

As consequências dessa disparidade para os direitos fundamentais são concretas. Mendes (2019) demonstra que a proteção de dados, elevada a direito fundamental autônomo pela EC 115/2022, exige instrumentos efetivos de tutela que a mera existência da norma não garante. A difusão dos dados em múltiplas jurisdições compromete direitos assegurados pela LGPD — acesso, retificação, portabilidade e, sobretudo, eliminação. Bioni (2019) já apontava que o modelo centrado no consentimento individual é insuficiente diante de relações assimétricas de poder como as que envolvem as grandes plataformas. Se o titular não identifica onde seus dados estão armazenados, seu direito de controlá-los torna-se inócuo. A isso se soma a dificuldade de responsabilização: quando uma violação envolve múltiplas jurisdições, a determinação da lei aplicável e da autoridade competente é problemática, gerando o que Kuner (2013) denomina vácuo sancionatório — um espaço entre jurisdições onde a responsabilidade se dilui.

11

Richards (2021), ao desenvolver o conceito de privacidade intelectual, oferece dimensão adicional: a privacidade não é apenas escudo contra intromissões, mas condição sistêmica para o exercício da liberdade de pensamento e do desenvolvimento intelectual autônomo. A vigilância corporativa compromete precisamente essa dimensão — e o *forum shopping*, ao permitir que as plataformas se situem em jurisdições de baixa proteção, agrava esse comprometimento ao torná-lo estrutural e sistemático.

Registre-se, por fim, que a análise aqui desenvolvida identifica a possibilidade teórica de arbitragem regulatória — os incentivos estruturais e os mecanismos pelos quais a fragmentação normativa pode favorecer as plataformas —, sem pretender demonstrar, empiricamente, a efetiva utilização dessas práticas por empresa específica, ressalva metodológica cujo alcance se detalha na seção de Métodos e se retoma na Conclusão. O *forum shopping* regulatório, portanto, não é abstração teórica: opera em camadas — societária, contratual e infraestrutural —, produz efeitos diretos sobre a proteção de dados e a autonomia digital de países como o Brasil, e revela

os limites de modelos regulatórios que não consideram a dimensão transnacional do poder das Big Techs.

3.3 Respostas Brasileiras: Avanços, Limites e Persistência

O ano de 2025 representou um ponto de inflexão na trajetória regulatória brasileira. Em junho, o Supremo Tribunal Federal, ao julgar o RE 1.037.396 (Tema 987), declarou a inconstitucionalidade parcial e progressiva do art. 19 do Marco Civil da Internet, impondo às plataformas digitais deveres proativos de moderação de conteúdo. Até então, o modelo brasileiro exigia ordem judicial prévia para responsabilização das plataformas por danos decorrentes de conteúdo de terceiros. Barroso (2022), ao examinar a tensão entre liberdade de expressão e regulação de plataformas, já sustentava a necessidade de um modelo de autorregulação regulada — no qual as plataformas mantêm autonomia operacional, mas submetem-se a deveres de transparência, devido processo e supervisão independente. O STF, em certa medida, acolheu essa direção ao determinar que grandes plataformas passassem a ter o dever de agir diante de conteúdos ilícitos, especialmente desinformação, discurso de ódio e violações a direitos fundamentais.

Essa virada jurisprudencial, contudo, não foi abrupta. Desde 2020, o STF vinha consolidando uma trajetória de afirmação dos direitos fundamentais no ambiente digital. Na ADI 6.387, relatoria da Ministra Rosa Weber, o Tribunal reconheceu a constitucionalidade da LGPD e afirmou a proteção de dados como direito fundamental autônomo, posição consolidada pela EC 115/2022.

Na ADPF 572 e nas ADIs 5.527 e 7.261, a Corte enfrentou questões relacionadas à liberdade de expressão, moderação de conteúdo e limites da responsabilidade das plataformas, construindo gradativamente o arcabouço interpretativo que desembocou no RE 1.037.396. Esse conjunto de decisões revela que o STF tem atuado como contrapeso institucional relevante diante do poder privado das grandes plataformas, ainda que a efetividade de suas decisões dependa de articulação entre os Poderes e as autoridades regulatórias — articulação que esbarra nos limites estruturais examinados adiante.

Na esteira dessa decisão, foram editados os Decretos nº 12.975 e 12.976/2026, que regulamentaram a nova interpretação constitucional e promoveram o fortalecimento da ANPD. Originalmente criada como órgão vinculado à Presidência com natureza de autarquia especial,

a ANPD teve suas competências ampliadas, com autonomia reforçada, poderes de fiscalização e apuração de infrações das plataformas e competência para auditar sistemas automatizados de decisão, nos termos do art. 20 da LGPD.

No mesmo período, foi sancionada a Lei nº 15.211/2025, que instituiu o Estatuto da Criança e do Adolescente Digital (ECA Digital). A lei estabelece regime de proteção específico para crianças e adolescentes no ambiente digital, reconhecendo que a vulnerabilidade desse grupo exige salvaguardas adicionais àquelas previstas na LGPD. Entre suas disposições, destacam-se a obrigatoriedade de design de plataformas adequado à idade, a proibição de tratamento de dados para perfil comportamental de crianças e a imposição de deveres de cuidado reforçados às plataformas. Sua pertinência para a hipótese deste estudo é direta: ao elevar o padrão protetivo para grupo especialmente vulnerável, o Estatuto depende, para ser eficaz, da capacidade estatal de impor a jurisdição nacional sobre plataformas estrangeiras — precisamente o ponto em que o *forum shopping* opera, ao dispersar infraestrutura, contratos e responsabilidade entre jurisdições. A edição do Estatuto reflete, ademais, o entendimento de que o modelo geral de proteção de dados, centrado no consentimento, mostra-se insuficiente diante da assimetria de poder entre plataformas e usuários quando se trata de grupos particularmente vulneráveis.

Esse conjunto normativo revela que o Brasil avançou significativamente na construção de um arcabouço jurídico voltado à proteção de dados e à afirmação da soberania digital. Todavia, a mera existência desse arcabouço não é suficiente para conter o *forum shopping*. Cohen (2019) adverte que o capitalismo informacional não é passivo diante da regulação: ele ativamente remodela as instituições jurídicas para neutralizar as restrições que lhe são impostas. Essa capacidade de adaptação institucional é particularmente aguda no caso das Big Techs, que dispõem de recursos financeiros, técnicos e jurídicos para explorar sistematicamente as lacunas entre o que a norma prevê e a capacidade fiscalizatória dos Estados.

A distância entre a norma editada e a efetividade concreta é estrutural, não acidental. A ANPD, mesmo após seu fortalecimento, registrou baixa atuação sancionatória no primeiro semestre de 2026. O problema, porém, não se reduz à insuficiência de pessoal ou orçamento. Há um desequilíbrio estrutural entre a autoridade fiscalizadora e as plataformas que a mera edição de normas não corrige. As Big Techs operam em dezenas de jurisdições simultaneamente, podem realocar recursos e dados entre países com custos relativamente baixos e têm capacidade

de litigar estrategicamente para postergar decisões regulatórias por anos. Cohen (2019) demonstra que o capitalismo informacional produz uma verdadeira "arquitetura da evasão": as plataformas estruturam suas operações em camadas geográficas e societárias precisamente para maximizar sua liberdade diante dos reguladores nacionais. Richards (2021), ao afirmar que a privacidade é sobre poder, oferece a chave para compreender que o *forum shopping* não é um efeito colateral indesejado da regulação, mas uma conduta deliberada de gestão do risco regulatório.

A isso se soma o fenômeno da captura regulatória em sua dimensão contemporânea. Na literatura especializada, a captura regulatória designa, em sua formulação clássica, o processo pelo qual o órgão regulador passa a atuar em favor dos interesses do setor regulado, em detrimento do interesse público. Diferentemente dessa captura clássica — baseada em lobby ou financiamento direto do regulador —, a captura no ambiente digital opera por meio do desequilíbrio informacional: as plataformas detêm conhecimento técnico muito superior ao dos órgãos reguladores sobre seus próprios sistemas, algoritmos e modelos de negócio, frequentemente resguardado por segredos de negócio.

Assunção (2025), ao analisar a opacidade algorítmica em suas dimensões técnica e legal, demonstra que essa assimetria de conhecimento não é acidental, mas estruturalmente produzida pelo próprio desenho dos sistemas e pela proteção jurídica conferida ao segredo empresarial. Essa disparidade torna a fiscalização intrinsecamente reativa e defasada — quando a ANPD consegue compreender uma prática, as plataformas já a modificaram. Esse descompasso estrutural entre a velocidade da inovação empresarial e a lentidão dos processos regulatórios é um dos fatores que tornam o *forum shopping* persistentemente eficaz. Moraes (2024), ao examinar o novo populismo digital extremista, adverte que a regulação de plataformas deve equilibrar o combate à desinformação com a proteção da liberdade de expressão — preocupação que se alinha às advertências de Floridi (2020) sobre os *trade-offs* inerentes às políticas de soberania digital.

O segundo fator estrutural que limita a eficácia das respostas brasileiras é a dependência infraestrutural. Como demonstra Cohen (2019), as regras legais e técnicas que governam os fluxos de informação estão estruturalmente desequilibradas: quando a infraestrutura física da internet — servidores, cabos submarinos, data centers e serviços de nuvem — é controlada por atores privados transnacionais, o poder regulatório dos Estados nacionais é intrinsecamente

limitado. Isso significa que órgãos públicos, empresas e instituições financeiras nacionais operam sobre infraestrutura cujo controle efetivo escapa à jurisdição brasileira. A soberania digital pressupõe não apenas a edição de leis, mas a capacidade técnica de fazê-las valer, e essa capacidade é severamente limitada quando a infraestrutura crítica de dados está em servidores estrangeiros. Pereira e Faleiros Júnior (2024) corroboram esse diagnóstico ao concluírem que a eficácia regulatória no Brasil esbarra em limites estruturais que a mera edição de normas não supera — entre eles, a captura regulatória, a assimetria de informações entre a autoridade e as empresas reguladas e a dificuldade de cooperação internacional.

A isso se soma a inexistência de uma decisão de adequação (*adequacy decision*) da União Europeia para o Brasil. Sem esse reconhecimento, as transferências internacionais de dados entre o bloco europeu e o país dependem de cláusulas contratuais padrão ou de outras salvaguardas, o que aumenta a complexidade e os custos de conformidade e reforça a posição periférica do Brasil no cenário global. Enquanto a Irlanda — sede europeia de diversas Big Techs — goza do privilégio de ser porta de entrada para o fluxo de dados no âmbito do GDPR, o Brasil permanece à margem desse circuito.

A persistência do *forum shopping*, portanto, não decorre de uma suposta inadequação das normas brasileiras, mas de fatores estruturais que transcendem a capacidade de resposta unilateral de qualquer Estado nacional. A captura regulatória informacional neutraliza a fiscalização antes mesmo de ela ocorrer; a dependência infraestrutural torna a aplicação das leis materialmente dependente de atores estrangeiros; a ausência de coordenação internacional efetiva permite às plataformas explorar os vácuos entre jurisdições; e o desequilíbrio de recursos entre o Estado e as Corporações torna a litigância estratégica um instrumento poderoso de postergação e erosão das decisões regulatórias.

Mendes (2019) e Ferreira (2020), ao analisarem os desafios institucionais da proteção de dados no Brasil, convergem quanto à necessidade de a ANPD dispor de instrumentos efetivos de fiscalização e auditoria como condição para que a norma se traduza em eficácia concreta. O que o Brasil fez até aqui — constitucionalizar a proteção de dados, fortalecer a ANPD, reinterpretar o Marco Civil, criar o ECA Digital — é relevante e necessário, mas insuficiente para romper o ciclo do *forum shopping*, cuja superação, como se verá, demanda medidas coordenadas de natureza institucional, internacional e tecnológica.

4. CONCLUSÃO

A sociedade digital, moldada pelo capitalismo de vigilância e pela governamentalidade algorítmica, reposicionou os dados pessoais como o ativo central da economia contemporânea — e, paradoxalmente, como o ponto mais vulnerável da arquitetura de direitos. Este artigo examinou a tensão entre o poder regulatório estatal e a atuação transnacional das grandes plataformas, tomando como fio condutor o *forum shopping* regulatório — categoria analítica que, como se precisou ao longo do texto, distingue-se do *forum shopping* judicial e da mera escolha de lei aplicável, por envolver a estruturação deliberada de operações societárias, contratuais e infraestruturais para se situar em jurisdições de ambiente normativo menos exigente. O percurso analítico partiu do diagnóstico de que a disparidade entre os marcos normativos não é um desvio conjuntural, mas uma condição típica do ambiente digital global, e buscou verificar em que medida essa heterogeneidade compromete a eficácia da LGPD e a afirmação da soberania digital brasileira.

A análise comparativa dos três principais regimes — GDPR, CCPA e LGPD — revelou que suas divergências não se limitam a graus variados de rigor normativo. Elas constituem um mosaico de regras concorrentes cuja heterogeneidade cria incentivos permanentes para que as Big Techs orientem suas operações societárias, contratuais e infraestruturais para as jurisdições menos exigentes. Essa arbitragem regulatória, como demonstraram Cohen (2019) e Richards (2021), não é um efeito colateral da regulação, mas uma estratégia deliberada de gestão do risco normativo, na qual o poder informacional busca neutralizar as contenções que os ordenamentos nacionais tentam impor. A fragmentação normativa global opera como condição de possibilidade para o *forum shopping* — fenômeno que, examinado em suas estratégias concretas, revela a dimensão estrutural do desafio à soberania digital de países periféricos como o Brasil.

Os mecanismos concretos de *forum shopping* examinados — a fragmentação societária, com escolha de sedes em jurisdições de regulação mais permissiva; a inserção de cláusulas de eleição de foro estrangeiro em contratos de adesão; e a dispersão geográfica da infraestrutura de dados — operam em camadas interligadas que se reforçam mutuamente. A arquitetura societária das grandes plataformas, com subsidiárias distribuídas entre países de baixa exigência regulatória, cria uma primeira barreira à responsabilização. A ela se somam os contratos de adesão, que frequentemente elegem tribunais estrangeiros e aplicam legislações com padrões

reduzidos de proteção, neutralizando instrumentos como o CDC e o CPC. No plano infraestrutural, o controle estrangeiro sobre a camada física da internet — servidores, cabos submarinos, data centers e serviços de nuvem — fragmenta a localização dos dados de modo a dificultar a aplicação de leis locais. A dependência brasileira de provedores estrangeiros de serviços em nuvem revelou-se, nesse quadro, o elo mais frágil da cadeia: sem capacidade tecnológica autônoma, a pretensão de soberania digital esbarra em um limite material que a edição de normas, por si só, não supera.

Em contrapartida, o Brasil avançou significativamente no plano normativo. A constitucionalização da proteção de dados como direito fundamental autônomo (EC 115/2022), a reinterpretação do art. 19 do Marco Civil pelo STF no RE 1.037.396 (Tema 987), o fortalecimento institucional da ANPD promovido pelos Decretos nº 12.975 e 12.976/2026 e a edição do ECA Digital (Lei nº 15.211/2025) representam um conjunto coerente e ambicioso de respostas institucionais aos desafios da regulação digital. Esse arcabouço, todavia, tem sua eficácia concretamente limitada por fatores que transcendem o texto normativo: a captura regulatória informacional, que opera pelo descompasso de conhecimento técnico entre regulador e regulado; o desequilíbrio de recursos entre uma autoridade nacional e corporações que atuam em dezenas de jurisdições simultaneamente; a dependência de provedores estrangeiros de nuvem, que torna a aplicação das leis materialmente dependente de atores sobre os quais o Estado brasileiro tem jurisdição limitada; e a ausência de coordenação internacional efetiva, que permite às plataformas explorar os vácuos entre ordenamentos jurídicos concorrentes.

O *forum shopping* regulatório, conforme demonstrado ao longo da análise, compromete parcialmente a eficácia da LGPD e a afirmação da soberania digital brasileira — mas não se trata de um quadro imutável. A hipótese inicial, de que seus efeitos podem ser mitigados por meio de três frentes complementares, encontrou respaldo na investigação. O fortalecimento institucional da ANPD é condição necessária, mas não suficiente: a autoridade precisa avançar de uma atuação reativa para uma fiscalização proativa, com capacidade de auditoria algorítmica e investigação autônoma que reduza o desequilíbrio informacional hoje existente. A formação de alianças regulatórias regionais e multilaterais — no âmbito do Mercosul, da CPLP e da Global Privacy Assembly — pode ampliar a capacidade de pressão do Brasil no cenário internacional e reduzir os incentivos à arbitragem entre jurisdições. Por fim, o desenvolvimento

progressivo de capacidade tecnológica autônoma, incluindo investimentos em infraestrutura de nuvem soberana e segurança cibernética, é a medida estrutural capaz de, a longo prazo, reduzir a dependência que hoje limita o alcance concreto das normas brasileiras.

Cabe registrar, com rigor metodológico, o alcance das conclusões aqui apresentadas. O presente estudo concentrou-se no *forum shopping* regulatório como estratégia de contorno das balizas normativas pelas Big Techs, identificando os incentivos estruturais e os mecanismos pelos quais a fragmentação normativa pode favorecer as plataformas — sem pretender demonstrar, empiricamente, a efetiva utilização dessas estratégias por empresa específica. A distinção entre a existência de incentivos e a comprovação de condutas concretas é essencial para situar o alcance da tese e evitar generalizações indevidas. Tampouco se pretendeu o *forum shopping* como o único instrumento de que essas corporações dispõem para evitar regulamentações estatais: estratégias como a captura regulatória via *lobby*, a litigância estratégica, a manipulação algorítmica, o uso abusivo de segredo de negócios, a exploração de lacunas fiscais e a concertação entre plataformas — embora igualmente relevantes e articuladas ao *forum shopping* em um ecossistema de evasão normativa que se retroalimenta — não foram objeto deste trabalho por opção metodológica deliberada. Incorporá-las diluiria o recorte analítico e comprometeria a profundidade da investigação, além de resultar em extensão incompatível com os limites de um artigo científico. A delimitação do objeto à arbitragem entre jurisdições como mecanismo central de elusão regulatória mostrou-se adequada para demonstrar, com a densidade necessária, a tese proposta.

A proteção de dados pessoais na era digital não é apenas uma questão técnica ou econômica — é, sobretudo, uma questão de cidadania. A possibilidade de controlar a própria informação, de conhecer os usos que dela se fazem e de resistir a formas de poder que operam pela opacidade algorítmica constitui condição elementar para o exercício da autonomia em ambiente digital. Como tal, exige do direito, da política e da tecnologia uma convergência de esforços que ainda está por ser plenamente construída. O desafio que se impõe às democracias contemporâneas é garantir que o ambiente digital não se converta em espaço de erosão de direitos, mas em um novo horizonte de afirmação da dignidade humana.

As limitações deste estudo sinalizam direções para investigações futuras. Pesquisas empíricas que acompanhem a atuação sancionatória da ANPD nos próximos anos poderão verificar se o fortalecimento institucional promovido pelos decretos de 2026 se traduz em

efetividade fiscalizatória ou se o desequilíbrio estrutural entre o órgão regulador e as empresas fiscalizadas persistirá independentemente do desenho normativo. Estudos comparativos que examinem o comportamento de plataformas específicas diante das reformas brasileiras, utilizando metodologias de rastreamento de fluxos de dados ou de análise de contratos de adesão, poderão oferecer evidências concretas sobre a magnitude do *forum shopping* setorial — preenchendo, assim, a lacuna empírica que este estudo, por sua natureza, não pôde suprir. Investigação aprofundada sobre o desenvolvimento de infraestrutura digital autônoma — nuvens soberanas, certificação de provedores locais, políticas de aquisição pública de tecnologia — pode contribuir para a formulação de estratégias de redução da dependência que hoje limita o alcance das normas brasileiras. Por fim, estudos que articulem direito, economia política e ciência da computação no exame da captura regulatória informacional podem lançar luz sobre mecanismos ainda pouco compreendidos de disparidade técnica entre reguladores e plataformas.

5. REFERÊNCIAS

ALVES, Marco Antonio Souza; ANDRADE, Otávio Morato de. Autonomia individual em risco? Governamentalidade algorítmica e a constituição do sujeito. *Cadernos Metrôpole*, 2022; 24(55): 1007-1023.

19

ASSUNÇÃO, Isadora Valadares. Segredo de negócios e decisões automatizadas discriminatórias: impasses e soluções regulatórias. In: AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS. III Prêmio Danilo Doneda de Artigos Científicos: artigos científicos vencedores. Brasília, DF: ANPD, 2025

BARROSO, Luna van Brussel. Liberdade de expressão e democracia na era digital: o impacto das mídias sociais no mundo contemporâneo. Belo Horizonte: Fórum, 2022.

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

BRASIL. Decreto nº 12.975, de 20 de maio de 2026. Altera o Decreto nº 8.771/2016 para regulamentar o Marco Civil da Internet. *Diário Oficial da União*, Brasília, DF, 20 maio 2026.

BRASIL. Decreto nº 12.976, de 20 de maio de 2026. Estabelece diretrizes para a proteção de mulheres na internet e para o enfrentamento da violência contra mulheres em ambiente digital. *Diário Oficial da União*, Brasília, DF, 20 maio 2026.

BRASIL. Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Altera a Constituição Federal para dispor sobre a proteção de dados pessoais. Diário Oficial da União, Brasília, DF, 11 fev. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

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

BRASIL. Lei nº 15.211, de 17 de setembro de 2025. Estatuto da Criança e do Adolescente Digital (ECA Digital). Diário Oficial da União, Brasília, DF, 18 set. 2025.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 5.527 Distrito Federal. Relatora: Ministra Rosa Weber. Julgada em maio 2020. Interpretação dos arts. 10 e 12 do Marco Civil da Internet.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 6.387 Distrito Federal. Relatora: Ministra Rosa Weber. Julgada em 7 maio 2020. Suspende a eficácia da Medida Provisória nº 954/2020.

BRASIL. Supremo Tribunal Federal. Ação Direta de Inconstitucionalidade 7.261 Distrito Federal. Relator: Ministro Edson Fachin. Julgada em 2023. Constitucionalidade da Resolução TSE 23.714/2022.

BRASIL. Supremo Tribunal Federal. Arguição de Descumprimento de Preceito Fundamental 572 Distrito Federal. Relator: Ministro Edson Fachin. Julgada em 18 jun. 2020. Declara a constitucionalidade do Inquérito 4.781.

BRASIL. Supremo Tribunal Federal. Recurso Extraordinário 1.037.396 São Paulo (Tema 987). Relator: Ministro Dias Toffoli. Julgado em 26 jun. 2025.

CALIFÓRNIA. California Consumer Privacy Act of 2018 (CCPA). California Civil Code §§ 1798.100-1798.199.100. Enacted June 28, 2018.

COHEN, Julie E. Between truth and power: the legal constructions of informational capitalism. New York: Oxford University Press, 2019.

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

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

FERREIRA, Rafael Freire. A Autoridade Nacional de Proteção de Dados – ANPD. In: LÓSSIO, C. J. B.; NASCIMENTO, L.; TREMEL, R. (Org.). Cibernética Jurídica: Estudos sobre Direito Digital. Campina Grande: EDUEPB, 2020.

FLORIDI, Luciano. The fight for digital sovereignty: what it is, and why it matters for the EU. *Philosophy & Technology*, 2020; 33: 369-378.

FRAZÃO, Ana; SANTOS, Luiza Mendonça da Silva Belo. Plataformas Digitais e o Negócio de Dados: Necessário Diálogo entre o Direito da Concorrência e a Regulação dos Dados. *Direito Público*, 2020; 17(93): 58-81.

GAILLARD, Emmanuel. *Legal Theory of International Arbitration*. Leiden: Martinus Nijhoff Publishers, 2010.

KUNER, Christopher. *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press, 2013.

LIM, Gabrielle. **The cost of control**: challenges and trade-offs of digital sovereignty. Waterloo: Centre for International Governance Innovation (CIGI), Digital Policy Hub, Working Paper, Fall 2025-2026. Disponível em: <https://www.cigionline.org/documents/3843/DPH-Paper-PolicyMemo-Lim.pdf>. Acesso em: 22 jul. 2026.

MENDES, Laura Schertel. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. *Panorama Setorial da Internet*, 2019; 11(2).

MORAES, Alexandre de. O Direito Eleitoral e o Novo Populismo Digital Extremista: liberdade de escolha do eleitor e a promoção da Democracia. 2024. Tese (Concurso de Professor Titular) — Faculdade de Direito, Universidade de São Paulo, São Paulo, 2024.

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

RICHARDS, Neil. *Why privacy matters*. Oxford: Oxford University Press, 2021.

ROUVROY, Antoinette; BERNS, Thomas. Governamentalidade algorítmica e perspectivas de emancipação: o díspar como condição de individuação pela relação? *Revista ECO-Pós*, 2015; 18(2): 139-163.

SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 2011; 86.

TUROBOV, Aleksei; CARRAPICO, Helena; FARRAND, Benjamin. Opening the Black Box of EU Digital Sovereignty: A Macro-Level Analysis of the Concept's Development. *Governance*, 2026. DOI: 10.1111/gove.70112.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (GDPR). *Jornal Oficial da União Europeia*, L 119, 4 maio 2016.

ZUBOFF, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: PublicAffairs, 2019.