

**SOBERANIA DIGITAL, DIREITOS SOCIAIS E ATUAÇÃO JUDICIAL EM
PROCESSOS REIVINDICATÓRIOS DE CONTROLE DE INFRAESTRUTURAS
DIGITAIS****DIGITAL SOVEREIGNTY, SOCIAL RIGHTS, AND JUDICIAL ACTION IN CLAIMS
FOR CONTROL OF DIGITAL INFRASTRUCTURES****SOBERANÍA DIGITAL, DERECHOS SOCIALES Y ACCIÓN JUDICIAL EN
DEMANDAS POR EL CONTROL DE INFRAESTRUTURAS DIGITALES****Luiz Fernando de Oliveira¹, Any Ávila Assunção²****RESUMO**

Este artigo investiga o impacto da soberania digital e do controle das infraestruturas tecnológicas sobre a efetivação dos direitos sociais em países em desenvolvimento, com foco no Brasil e em casos demandados perante o Supremo Tribunal Federal. A crescente dependência de infraestruturas digitais controladas por empresas internacionais, como a plataforma "X", a Meta e a Google levanta preocupações sobre a capacidade do Estado de implementar políticas públicas em áreas essenciais como educação, saúde e segurança. A partir da análise do conceito de soberania digital, este estudo explora os desafios dessa dependência, as consequências para a autonomia estatal, e os riscos que isso representa para a justiça social. O artigo também examina o papel dos grandes grupos econômicos no controle dessas infraestruturas e discute como a falta de uma soberania digital plena perpetua desigualdades, limitando o acesso a direitos sociais. Ao final, discute a necessidade de o Brasil adotar estratégias que fortaleçam seu controle tecnológico para promover um ecossistema digital mais justo e inclusivo, capaz de garantir a reivindicação e efetivação dos direitos sociais.

Palavras-chave: Soberania Digital. Direitos Sociais. Infraestruturas Digitais. Políticas Públicas. Inclusão Digital. Justiça Social.

ABSTRACT

This paper examines the implications of digital sovereignty and the control of technological infrastructures on the realization of social rights in developing countries, with a particular focus on Brazil. By analyzing the concept of digital sovereignty, the study explores the challenges posed by the growing dependence on digital infrastructures controlled by multinational corporations, and the subsequent implications for state autonomy and social justice. Through a case study of Brazil and an analysis of cases brought before the Supreme Federal Court, this research highlights the risks associated with this dependency, including the potential for increased inequality and limited access to social rights. The paper concludes by discussing the need for Brazil to develop strategies to strengthen its technological control and promote a more equitable and inclusive digital ecosystem.

Recibido: 12/08/2024 | Aceptado: 12/09/2024 | Publicación en línea: 11/11/2024.



Esta obra está bajo una [Licencia Creative Commons Atribución- NoComercial 4.0 Internacional](https://creativecommons.org/licenses/by-nc/4.0/)

¹ Doutor em História do Direito, Instituto de Educação Superior de Brasília (IESB), Brasília, Distrito Federal, Brasil.
E-mail: luizfernandokerix@gmail.com Orcid: <https://orcid.org/0000-0003-4275-1817>

² Doutora em Sociologia Jurídica, Instituto de Educação Superior de Brasília (IESB), Brasília, Distrito Federal, Brasil.
E-mail: any.assunção@iesb.br Orcid: <https://orcid.org/0000-0003-2125-4037>

Keywords: Digital Sovereignty. Social Rights. Digital Infrastructures. Public Policies. Digital Inclusion. Social Justice.

RESUMEN

Este trabajo examina las implicaciones de la soberanía digital y el control de las infraestructuras tecnológicas en la realización de los derechos sociales en países en desarrollo, con un enfoque particular en Brasil. Al analizar el concepto de soberanía digital, el estudio explora los desafíos planteados por la creciente dependencia de infraestructuras digitales controladas por corporaciones multinacionales, y las subsiguientes implicaciones para la autonomía estatal y la justicia social. A través de un estudio de caso de Brasil y un análisis de casos presentados ante el Supremo Tribunal Federal, esta investigación destaca los riesgos asociados con esta dependencia, incluyendo el potencial de aumento de la desigualdad y el acceso limitado a los derechos sociales. El documento concluye discutiendo la necesidad de que Brasil desarrolle estrategias para fortalecer su control tecnológico y promover un ecosistema digital más equitativo e inclusivo.

Palabras clave: Soberanía Digital. Derechos Sociales. Infraestructuras Digitales. Políticas Públicas. Inclusión Digital. Justicia Social.

INTRODUÇÃO

O surgimento da era digital transformou significativamente as relações jurídicas, sociais, políticas e econômicas em todo o mundo. Com a criação e aperfeiçoamento das tecnologias da informação e comunicação, o digital tornou-se um tema central para a execução de políticas públicas, principalmente em países em desenvolvimento, como é o caso do Brasil. Ocorre que essa crescente dependência de infraestruturas digitais controladas por grandes corporações internacionais levanta pontos de atenção importantes sobre a soberania digital e a efetivação dos direitos sociais, uma vez que o acesso e o controle dessas infraestruturas não apenas condicionam a implementação de serviços essenciais, mas também configuram um novo espaço de disputa por justiça social, direitos fundamentais e direitos sociais.

A soberania, tema clássico na teoria do Estado (Costa, 2020), em sua perspectiva digital, refere-se à capacidade de um Estado de controlar suas próprias infraestruturas tecnológicas e a gestão dos dados de seus cidadãos, permitindo que as políticas públicas sejam moldadas de acordo com as necessidades e especificidades locais (Lemos, 2015). No entanto, a realidade brasileira é marcada por uma dependência significativa de tecnologias desenvolvidas e geridas por empresas estrangeiras, o que compromete a autonomia do país em diversas áreas, incluindo educação, saúde e segurança pública. A falta de controle sobre essas tecnologias não apenas limita a eficácia das políticas sociais, mas também expõe os cidadãos a riscos de violação de direitos, como privacidade e proteção de dados pessoais (Barroso, 2024).

Isto posto, o intuito deste texto é investigar como a soberania digital e o controle das infraestruturas tecnológicas impactam o acesso e a efetivação de direitos sociais no Brasil,

especialmente considerando as discussões judiciais que têm sido travadas no Brasil perante o Supremo Tribunal Federal em decisões de ministros que são tendentes a reafirmar a soberania digital, causando um desconforto perante certos segmentos empresariais e adeptos de ideologias e partidos políticos. A análise parte da premissa de que a dependência de tecnologias estrangeiras não é um mero desafio técnico, mas uma questão política e social que afeta diretamente a justiça e a inclusão (Oliveira, 2018). A justificativa para este estudo reside na urgência de compreender como o controle das infraestruturas digitais pode se tornar um vetor de transformação social e uma ferramenta para a promoção da justiça social em um cenário onde a autonomia do Estado brasileiro se encontra em risco.

A problemática que surge neste contexto pode ser sintetizada por meio dos seguintes questionamentos: em que medida a dependência de infraestruturas digitais controladas por grandes corporações pode afetar a autonomia dos Estados na garantia de direitos sociais? Como o Estado brasileiro tem se posicionado diante de sua soberania digital? As políticas públicas voltadas à tecnologia e os aparatos legislativos do Brasil têm sido suficientes?

Para abordar essa problematização, a estrutura deste texto está organizada em cinco tópicos. O primeiro aborda o conceito de soberania digital e sua relevância no contexto brasileiro. Em seguida, explora os desafios impostos pela dependência tecnológica e as consequências para a autonomia do Estado. Depois, examina o papel das corporações estrangeiras na configuração desse cenário de dependência. Após, analisa os impactos dessa situação na efetivação dos direitos sociais no Brasil, discutindo, inclusive, decisões judiciais do Supremo Tribunal Federal que têm sido consideradas polêmicas. Por fim, discute medidas afirmativas relacionadas à soberania digital.

A realização desta pesquisa é consequência da produção e das reflexões acadêmicas que se iniciaram por ocasião do doutoramento de um dos autores do texto, onde foi possível abordar a tese do direito ao esquecimento e suas implicações para o controle de infraestruturas digitais. Assim, seguem as reflexões a seguir para se pensar sobre um tema que envolve o direito e mudanças sociais cuja tecnologia se pauta como alicerce.

METODOLOGIA

A metodologia deste artigo consiste em uma abordagem qualitativa e exploratória, focada em uma análise teórica e bibliográfica sobre o tema da soberania digital e sua interface com a comunicação e os direitos sociais no Brasil. Partindo de um levantamento de obras acadêmicas,

documentos legislativos e relatórios internacionais, a pesquisa busca delinear os principais conceitos e perspectivas teóricas sobre a soberania digital e sua relação com o controle estatal das infraestruturas tecnológicas. São analisados dados sobre políticas públicas, regulamentações internacionais e a atuação das Big Techs para compreender como essas questões impactam a autonomia comunicacional e a efetivação dos direitos sociais no contexto brasileiro.

A primeira etapa consiste em realizar um levantamento bibliográfico em bases de dados acadêmicas, como Scopus, Web of Science, SciELO e Google Scholar, além de legislações nacionais e internacionais. Esse levantamento visa identificar as principais obras e estudos recentes que tratam dos conceitos de soberania digital, direitos sociais e regulação das infraestruturas digitais. Autores reconhecidos nas áreas de comunicação digital, governança da internet e proteção de dados pessoais, como Barroso (2024), Doneda (2020) e Polido (2024), servirão de base teórica para o desenvolvimento da argumentação. A análise dessas fontes permitirá estabelecer uma base sólida sobre as discussões já existentes e as lacunas identificadas pela literatura.

Em uma segunda fase, o artigo utiliza uma análise documental de legislações e regulamentações relevantes ao tema, como o Marco Civil da Internet, a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia. Essa análise tem o propósito de identificar as diretrizes que buscam garantir a proteção de dados e o controle sobre infraestruturas tecnológicas no Brasil e em outros países. Além disso, serão examinadas as estratégias e os marcos regulatórios adotados pela China e União Europeia, como o Grande Firewall e o projeto Gaia-X, para avaliar como esses modelos podem influenciar o desenvolvimento de políticas públicas de soberania digital no Brasil. A metodologia inclui ainda uma abordagem comparativa entre os contextos de soberania digital em diferentes países, destacando os contrastes entre modelos de governança e comunicação das infraestruturas digitais.

A análise qualitativa dos dados coletados é guiada pela técnica de análise de conteúdo. Essa técnica permite categorizar os dados em temas e subtemas, de acordo com os principais eixos de discussão identificados na revisão bibliográfica e na análise documental. Assim, é possível identificar as principais tendências, desafios e oportunidades para o fortalecimento da soberania digital no Brasil, além de compreender como a comunicação entre as infraestruturas tecnológicas e a sociedade impacta a autonomia nacional no cenário global.

Por fim, a metodologia também abrange a construção de um panorama crítico que identifique as lacunas e possíveis avanços nas políticas de soberania digital no Brasil, com base na análise comparativa e nos resultados das revisões bibliográfica e documental. Este panorama

é essencial para propor estratégias que fortaleçam a autonomia digital do país, promovam a proteção dos direitos sociais e garantam uma comunicação democrática e acessível, mesmo diante do controle das grandes corporações de tecnologia.

Essa abordagem metodológica permite que o trabalho aqui formulado construa uma análise aprofundada e abrangente do estado atual da soberania digital no Brasil e sua relação com os direitos sociais. Dessa forma, o artigo contribui com subsídios para a formulação de políticas públicas e estratégias de regulação que assegurem a independência e a segurança das infraestruturas digitais brasileiras, fortalecendo o controle nacional sobre dados e comunicações no contexto digital global.

CONCEITO DE SOBERANIA DIGITAL E INFRAESTRUTURAS TECNOLÓGICAS

Em termos conceituais, a soberania digital pode ser entendida como a capacidade de um Estado exercer controle sobre seus recursos digitais, infraestruturas e dados de seus cidadãos, sem depender de protagonistas internacionais. Essa ideia adquire importância em um mundo cada vez mais interconectado, cujo acesso a tecnologias digitais é fundamental para a economia, segurança, direitos sociais e processos reivindicatórios. Ao partir das pesquisas de autores como Lemos (2015), Pinto (2018) e Cintra (2023), constata-se que a soberania digital está diretamente ligada à independência do Estado em relação à governança tecnológica internacional, principalmente no que diz respeito aos grandes grupos econômicos que possuem o controle das infraestruturas digitais globais. Para além das infraestruturas físicas, o conceito de soberania digital abrange o controle sobre o fluxo de informações e a regulamentação de plataformas digitais (WOODS, 2023).

As infraestruturas tecnológicas que amparam o ambiente digital moderno envolvem redes de telecomunicações, servidores, data centers, plataformas de software, serviços de nuvem e redes sociais. Boa parte dessas infraestruturas está sob o controle de empresas multinacionais, como Amazon Web Services (AWS), Google, "X" e Microsoft, o que restringe o poder dos Estados em garantir o domínio sobre dados sensíveis e a própria autonomia tecnológica.

No Brasil, Polido (2024) adverte que essa dependência tecnológica põe em risco a segurança de informações públicas e a privacidade dos cidadãos, e ainda dificulta a implementação de políticas públicas efetivas, pois, mesmo com avanços regulatórios, o Brasil ainda é altamente dependente de plataformas estrangeiras para comunicação digital, dificultando a soberania plena no ambiente digital (Rocha, 2024). Essa discussão passa pelo Marco Civil da

Internet, que estabelece direitos e deveres no uso da rede mundial de computadores (Brasil, 2014).

Outro aspecto relevante é a crescente necessidade de desenvolvimento de infraestruturas digitais próprias para proteger os interesses nacionais, especialmente em um cenário global de acirramento das disputas pelo controle dos dados e da tecnologia. Países como a China e a União Europeia têm adotado estratégias robustas para garantir sua soberania digital.

Na China, por exemplo, o governo tem investido maciçamente no desenvolvimento de infraestruturas tecnológicas locais e no controle rigoroso sobre as empresas de tecnologia que atuam no país. Segundo Xinxchuchu (2022), a criação de redes de servidores próprios, o desenvolvimento de tecnologias de inteligência artificial e a imposição de barreiras regulatórias para empresas estrangeiras são algumas das medidas adotadas pelo governo chinês para proteger seus dados e infraestrutura digital.

De forma semelhante, a União Europeia tem se destacado pela criação de regulamentações rígidas voltadas à proteção de dados e pela promoção de uma infraestrutura digital independente. Normativas como o Regulamento Geral sobre a Proteção de Dados (GDPR) são um dos exemplos de como o bloco busca proteger as informações dos seus cidadãos e garantir que as empresas que operam na Europa respeitem suas regras de privacidade e segurança digital. Além disso, a UE vem investindo em tecnologias locais e promovendo iniciativas para reduzir a dependência de grandes corporações estrangeiras, como apontam König e Müller (2024). Nesse contexto, existe previsão de investimentos significativos em inovação tecnológica e infraestrutura digital, reforçando a busca por uma maior soberania digital no continente.

Esses exemplos demonstram como a construção de infraestruturas próprias e a criação de marcos regulatórios robustos são essenciais para a proteção dos interesses nacionais no contexto digital, e servem como inspiração para o Brasil no desenvolvimento de políticas públicas voltadas à efetivação de direitos sociais em um ambiente de soberania digital.

Marques (2020), ao estudar o quadro brasileiro, sinaliza a falta de uma estratégia específica para o desenvolvimento de tecnologias nacionais, ressaltando que o país ainda precisa de um plano robusto para diminuir sua dependência de infraestruturas digitais internacionais. Para além do controle físico das infraestruturas, a soberania digital também abrange a capacidade de um Estado regulamentar e proteger o fluxo de dados que circula em seu próprio território. Em termos globais, dados se transformam em recursos estratégicos, comparáveis ao petróleo e metais preciosos, sendo utilizados pelo mundo corporativo e governos para exercer influência sobre políticas públicas, decisões econômicas, comportamentos sociais e processos reivindicatórios (Costa, 2020).

Shoshana Zuboff (2021), em sua obra "A Era do Capitalismo de Vigilância", investiga como a concentração do poder de processamento e armazenamento de dados em empresas estrangeiras enfraquece a capacidade do Estado de regular de forma eficaz esse fluxo, comprometendo a soberania digital e, por consequência, a capacidade de efetivar direitos sociais fundamentais. A concentração de poder digital em grupos econômicos internacionais restringe, inclusive, a capacidade dos países de implementarem políticas públicas eficazes direcionadas para os direitos sociais. Infraestruturas digitais como plataformas educacionais, dentre as quais a BlackBoard, sistemas de saúde digital e até iniciativas de segurança pública e bancária dependem, muitas vezes, de tecnologias e servidores controlados fora das fronteiras nacionais. Essa dependência compromete a autonomia do Brasil na criação de soluções tecnológicas que valorizem os interesses nacionais e acompanhem as necessidades sociais de maneira justa e soberana, o que resulta em uma vulnerabilidade estrutural do país (Pellegrini, 2023).

Uma outra dimensão da soberania digital diz respeito à capacidade de um Estado desenvolver alternativas nacionais para tecnologias essenciais, como redes sociais, plataformas de streaming e sistemas de pagamento digital. O problema se evidencia no fato de que a criação de alternativas é impactada pela ausência de investimentos em pesquisa e desenvolvimento tecnológico, especialmente em universidades públicas, agências de fomento e outras instituições de pesquisa que financiam a produção científica e tecnológica do Brasil. Como argumenta Danilo Doneda (2020), o país tem enfrentado dificuldades em competir globalmente, devido à falta de incentivos para o desenvolvimento de tecnologias próprias e à dependência crônica de soluções estrangeiras, o que afeta diretamente sua soberania no campo digital. Dessa forma, a soberania digital não é apenas uma questão de controle físico das infraestruturas digitais, mas também de controle sobre os fluxos de dados e a capacidade de um Estado em proteger os interesses de sua população no ambiente digital. A criação de políticas públicas que garantam o controle nacional sobre essas infraestruturas e dados torna-se crucial para a promoção de direitos sociais, como saúde, educação e segurança, e seus processos reivindicatórios, em um mundo cada vez mais digitalizado.

Nessa linha, Polido (2021; 2024) enfatiza a necessidade de fortalecer as capacidades nacionais para garantir que o Brasil possa exercer seu poder soberano de forma plena no ambiente digital, promovendo, assim, justiça e equidade no acesso aos direitos sociais.

IMPACTOS DO CONTROLE EXTERNO SOBRE DIREITOS SOCIAIS

A soberania nacional na garantia de direitos sociais está cada vez mais ameaçada pela dependência de infraestruturas digitais controladas por empresas estrangeiras. A educação, a saúde e a segurança, pilares do bem-estar social, estão sendo moldadas por algoritmos e decisões tomadas fora do país. Essa situação compromete a capacidade do Estado brasileiro de definir e implementar políticas públicas que atendam às necessidades específicas da população, além de gerar riscos para a segurança nacional e a privacidade dos cidadãos (Antunes, 2017).

No campo da educação, a digitalização de processos educacionais, principalmente durante a pandemia de COVID-19, evidenciou a dependência de plataformas internacionais, como a Google Classroom, Google Meet, BlackBoard e Microsoft Teams. Embora essas ferramentas tenham viabilizado o ensino remoto, elas também puseram o Brasil em uma posição de dependência tecnológica, onde dados educacionais de milhões de alunos e professores foram armazenados em servidores fora do país. Isso não só compromete a soberania digital, mas também impacta diretamente a privacidade e a segurança dos usuários, e ainda, deteriora gradualmente a capacidade de o Brasil controlar seu próprio sistema educacional digital, deixando o país à mercê das decisões comerciais e estratégicas de empresas estrangeiras (BELLI ET ALL, 2023).

O setor de saúde também enfrenta desafios significativos em termos de soberania digital. As tecnologias utilizadas para o armazenamento de dados de pacientes, telemedicina e gestão de sistemas hospitalares, muitas vezes, dependem de soluções internacionais. A falta de controle sobre esses sistemas compromete a capacidade de o Estado garantir a privacidade dos dados dos pacientes e a integridade dos serviços de saúde pública. De acordo com Koerner (2021), essa dependência pode gerar graves consequências, incluindo a interrupção de serviços essenciais em caso de falhas ou mudanças unilaterais nas políticas das empresas que controlam as infraestruturas tecnológicas. Essa vulnerabilidade afeta o acesso igualitário à saúde, um direito social garantido pela Constituição Federal.

Na segurança pública, bancária e financeira, a soberania digital também desempenha um papel crucial. As tecnologias de vigilância, controle e monitoramento de crimes dependem cada vez mais de sistemas digitais que, boa parte das vezes, são operados por empresas estrangeiras. Isso permite a construção de um cenário em que dados sensíveis brasileiros, incluindo informações biométricas, podem ser acessados por pessoas de outros países, comprometendo não apenas a privacidade, mas também a segurança nacional. Pellegrini (2023) alerta para os riscos de um Estado perder o controle sobre suas infraestruturas de segurança, destacando que o uso de

tecnologias estrangeiras nesses setores pode limitar a capacidade do Brasil de gerenciar suas próprias políticas de segurança de forma independente.

A dependência de infraestruturas digitais estrangeiras não é apenas uma questão tecnológica, mas também política, jurídica e social, pois afeta diretamente a capacidade de o Estado garantir o acesso igualitário aos direitos sociais e seus processos reivindicatórios. Quando um país perde o controle sobre suas infraestruturas digitais, ele se vê incapaz de implementar políticas públicas de forma soberana, tornando-se vulnerável a interferências externas e limitações tecnológicas. Com isso, o desafio que o Brasil enfrenta é o de desenvolver um arcabouço tecnológico nacional que permita garantir a efetivação de direitos sociais sem depender de sujeitos internacionais, fortalecendo, dessa forma, a autonomia do Estado.

MODELOS DE SOBERANIA DIGITAL

As grandes corporações estrangeiras, como Google, Amazon, Microsoft, "X" e Facebook (Meta), possuem uma função importante na estrutura tecnológica mundial. A influência dessas empresas não se restringe somente à esfera econômica, mas também abrange aspectos políticos e sociais, principalmente em países em desenvolvimento. No caso do Brasil, a dependência das soluções tecnológicas oferecidas por essas corporações internacionais impacta diretamente a capacidade do Estado de exercer controle sobre setores estratégicos, como telecomunicações, processamento de dados e serviços públicos digitais.

Para Bioni (2018), essa dependência cria assimetrias de poder que colocam o país em posição de vulnerabilidade frente aos interesses comerciais desses grupos econômicos, que muitas vezes são conflitantes com os objetivos nacionais de soberania e justiça social.

Considerando que muitos serviços públicos, como educação e saúde, dependem de infraestruturas tecnológicas desenvolvidas por essas empresas, a autonomia do Brasil para implementar políticas públicas se vê ameaçada. A capacidade de exercer controle sobre dados sensíveis de sua população é, assim, fortemente limitada. Um exemplo disso é a dependência dos serviços de computação em nuvem, onde dados de cidadãos brasileiros são armazenados em servidores localizados fora do território nacional, o que impede o controle total dessas informações pelo Estado. O modelo de soberania digital, portanto, pressupõe a construção de uma infraestrutura nacional de tecnologia, incluindo servidores, plataformas e regulamentos voltados para a proteção de dados e a segurança das informações. Polido (2024) sugere que o Brasil deve buscar inspiração em modelos internacionais, como o europeu e o chinês, que priorizam o

controle local de infraestruturas críticas. A União Europeia, com o GDPR, e a China, com sua política de “grande firewall”, são exemplos de como a soberania digital pode ser promovida de forma a proteger os interesses nacionais e garantir que os serviços públicos sejam administrados com base nas necessidades locais e com autonomia tecnológica.

A presença de grupos econômicos externos na infraestrutura digital do Brasil se dá de maneira pujante e deve ser vista com cautela, pois a maioria dos serviços de computação em nuvem, armazenamento de dados e plataformas digitais estão sendo controlados por empresas internacionais.

Por exemplo, sistemas que gerenciam dados sensíveis da população brasileira no setor público, como cadastros de saúde e segurança, inúmeras vezes utilizam servidores de empresas como Amazon Web Services (AWS) e Google Cloud. Essa situação compromete a soberania nacional, pois os dados ficam sujeitos às legislações dos países onde essas empresas estão sediadas, como se pode observar nas leis e estratégias de vigilância dos Estados Unidos da América (THE WHITE HOUSE WASHINGTON, 2023). Considerando a posição estadunidense, essa estratégia permite que o governo tenha acesso a dados armazenados em servidores de empresas dos EUA, independentemente de onde esses dados estejam localizados, o que representa um risco para a soberania brasileira.

Outro aspecto preocupante é a influência política e econômica que esses grandes e poderosos grupos econômicos exercem sobre os governos. As grandes multinacionais de tecnologia possuem recursos financeiros e lobby suficiente para moldar legislações a seu favor, dificultando a criação de políticas públicas que favoreçam a soberania digital. Essas empresas atuam como intermediárias essenciais no processo de digitalização de serviços, ao mesmo passo em que criam uma dependência que impede o desenvolvimento de soluções tecnológicas nacionais. Apesar de parecerem agentes neutros, as *Big Techs* têm interesses econômicos e geopolíticos próprios, que podem entrar em conflito com os objetivos nacionais de desenvolvimento e justiça social (Koerner, 2021).

Além do controle direto sobre as infraestruturas tecnológicas, as corporações estrangeiras também moldam o comportamento social e econômico dos cidadãos brasileiros por intermédio de suas plataformas. Redes sociais, como Facebook, Instagram e TikTok moldam o fluxo de informação e influenciam o debate público. O controle que essas empresas possuem sobre o conteúdo publicado em suas plataformas permite a censura, a manipulação de algoritmos e o direcionamento de propagandas, o que pode impactar diretamente os direitos à liberdade de expressão e à privacidade dos usuários. Com isso, a falta de regulamentação específica para essas

plataformas no Brasil permite que essas corporações utilizem suas tecnologias para fins comerciais que podem prejudicar a efetivação de direitos sociais e a própria democracia (Pellegrini, 2023).

As grandes corporações são protagonistas da revolução digital, mas a falta de uma base tecnológica própria no Brasil nos torna meros consumidores de suas soluções. Para construir uma soberania digital, precisamos estimular a inovação nacional, investindo em pesquisa e desenvolvimento e criando um ecossistema favorável à emergência de empresas brasileiras capazes de competir no mercado global, conforme será discutido a seguir.

POLÍTICAS PÚBLICAS PARA SOBERANIA DIGITAL E EFETIVAÇÃO DOS DIREITOS SOCIAIS: PROCESSOS REIVINDICATÓRIOS PERANTE O SUPREMO TRIBUNAL FEDERAL

A soberania digital está intrinsecamente ligada à capacidade de os países controlarem suas infraestruturas tecnológicas para garantir a efetivação dos direitos sociais. No Brasil, onde os serviços públicos dependem cada vez mais de plataformas digitais, a falta de soberania digital compromete a implementação de direitos sociais essenciais, como educação, saúde e segurança pública. Esses direitos, previstos na Constituição Federal de 1988, demandam que o Estado tenha controle sobre as infraestruturas tecnológicas que sustentam os serviços que os asseguram. Caso os dados e serviços estejam centralizados nas mãos de empresas internacionais, o governo brasileiro fica impedido de ter um maior domínio sobre o desenvolvimento, bem como fica limitado na elaboração e manutenção de políticas públicas voltadas à inclusão social.

Na área da educação, por exemplo, a crescente digitalização do ensino, especialmente após a pandemia de COVID-19, evidenciou a dependência das plataformas digitais internacionais, como Google Classroom, BlackBoard e Microsoft Teams. A falta de uma infraestrutura educacional digital nacional coloca em risco a autonomia do Estado em implementar políticas educacionais inclusivas, já que grande parte do conteúdo educacional e dos dados de estudantes são gerenciados por empresas privadas.

Para Sérgio Amadeu da Silveira e Tarcízio Silva (2024), a ausência de uma plataforma educacional pública e soberana contribui para a perpetuação das desigualdades, já que muitas escolas e instituições de ensino em áreas vulneráveis dependem de soluções tecnológicas que não são acessíveis a todos. Essa dependência tecnológica afeta o direito à educação de qualidade (SILVA, 2005), previsto no artigo 205 da Constituição, e perpetua a exclusão digital de

comunidades marginalizadas.

Na área da saúde, o uso de plataformas estrangeiras para o armazenamento e processamento de dados de pacientes compromete a privacidade e a segurança das informações pessoais dos cidadãos. No Brasil, os sistemas de saúde pública, como o SUS (Sistema Único de Saúde), dependem de infraestruturas digitais para a gestão de cadastros e a oferta de serviços de telemedicina. No entanto, boa parte desses dados sensíveis é armazenada em servidores controlados por empresas estrangeiras (Silva, 2022). A soberania digital é essencial para garantir a privacidade dos cidadãos e a segurança das informações de saúde, especialmente diante de legislações estrangeiras que podem permitir o acesso a esses dados por governos e corporações externas, comprometendo o direito à saúde e à privacidade, assegurados nos artigos 6º e 196 da Constituição (Brasil, 1988; Barroso, 2024).

Outro direito social diretamente impactado pela falta de soberania digital é o direito à segurança, seja ela pública, bancária ou financeira. A crescente adoção de tecnologias de vigilância digital, como câmeras de monitoramento e sistemas de reconhecimento facial, traz novos desafios ao controle estatal sobre a proteção da privacidade dos cidadãos. A utilização de soluções tecnológicas fornecidas por empresas estrangeiras, como câmeras conectadas à internet e algoritmos de análise de dados, coloca as informações sensíveis dos brasileiros e estrangeiros em solo brasileiro em uma posição de vulnerabilidade. A dependência de soluções externas para garantir a segurança pública abre espaço para o uso inadequado de dados e possíveis violações aos direitos fundamentais, como o direito à privacidade e à liberdade individual, garantidos pela Constituição da República Federativa do Brasil em seus artigos 5º e 6º. A ausência de uma infraestrutura digital soberana, portanto, não só impede o país de exercer controle sobre suas políticas públicas, mas também afeta diretamente a inclusão social. A dependência das plataformas tecnológicas internacionais cria um ciclo de desigualdade, onde os cidadãos com menos acesso às tecnologias e à internet de qualidade são marginalizados dos benefícios das políticas públicas digitais (Doneda, 2011).

A soberania digital é um fator essencial para garantir que os direitos sociais sejam efetivados de forma equitativa, possibilitando que todos os cidadãos tenham acesso igualitário aos serviços públicos e às oportunidades de inclusão digital. Sem o controle sobre essas infraestruturas, o Brasil corre o risco de perpetuar as desigualdades sociais já existentes, dificultando o acesso justo e igualitário aos direitos fundamentais (Silva, 2005).

O Supremo Tribunal Federal (STF) tem desempenhado um papel crucial na modulação da relação entre as plataformas digitais, os direitos sociais e a soberania digital no Brasil (Barroso,

2024). As decisões da corte envolvendo o WhatsApp e, mais recentemente, a rede social X (antigo Twitter), evidenciam a complexidade desse debate e a necessidade de um equilíbrio entre a liberdade de expressão, a privacidade e o cumprimento das leis nacionais.

As primeiras grandes decisões do STF envolvendo plataformas digitais tiveram como protagonista o WhatsApp, representada aqui pela ADPF 403 (STF, 2017). A controvérsia se iniciou com a discussão sobre a quebra de sigilo de dados armazenados no exterior, levantando questões decisivas sobre a aplicação da legislação brasileira em um ambiente globalizado e a proteção da privacidade dos usuários. O STF, em diversas oportunidades, reafirmou a importância da proteção dos dados pessoais e a necessidade de que as plataformas digitais cooperem com as investigações, desde que devidamente fundamentadas e autorizadas judicialmente, como acontece com a aplicação da tese do direito ao esquecimento (Oliveira, 2018). Essas decisões demonstraram a preocupação da corte em garantir a efetividade das investigações criminais, sem comprometer os direitos fundamentais dos usuários (Barroso, 2024).

Mais recentemente, o STF voltou a se debruçar sobre a regulação das plataformas digitais, desta vez com foco na rede social "X", representada pela análise da "Petição 12.404 Distrito Federal" (STF, 2024). A suspensão temporária da conta do presidente da República, imposta pela plataforma, gerou um intenso debate sobre a liberdade de expressão, a neutralidade da rede e o poder moderador das plataformas. O STF, ao analisar o caso, reafirmou a importância da liberdade de expressão e da neutralidade da rede, mas também destacou a responsabilidade das plataformas digitais em combater a disseminação de discursos de ódio, fake news e outras formas de abuso. A corte, ao determinar o desbloqueio da conta, ressaltou a necessidade de um diálogo entre as plataformas, o Estado e a sociedade civil para a construção de um ambiente digital mais seguro e democrático.

As decisões do STF sobre o WhatsApp e a rede social "X" demonstram a relevância da soberania digital para a proteção dos direitos sociais no Brasil. A soberania digital se refere à capacidade do Estado de regular o espaço digital, garantindo a segurança nacional, a proteção dos direitos fundamentais e o desenvolvimento econômico e social (LEMOS, 2015). Ao exigir que as plataformas digitais cumpram as leis brasileiras e respeitem os direitos dos usuários, o STF contribui para a construção de um ambiente digital mais justo e equitativo. Essa atuação da corte demonstra a necessidade de um equilíbrio entre a liberdade de expressão e a proteção de outros direitos fundamentais, como a privacidade, a honra e a imagem (Barroso, 2024).

Ou seja, a atuação do STF na regulação das plataformas digitais é fundamental para a construção de uma sociedade mais justa e democrática no mundo digital, ainda que essa postura

desagrade tanto empresas e grupos econômicos, bem como cidadãos e partidos políticos que defendem uma ideologia de Estado mínimo e postura não intervencionista em questões econômicas. As decisões da corte sobre o WhatsApp e a rede social "X" demonstram a complexidade desse debate e a necessidade de um diálogo constante entre os diferentes atores envolvidos.

MEDIDAS AFIRMATIVAS DE SOBERANIA DIGITAL

A soberania digital é indispensável para que o Brasil consiga efetivar os direitos sociais de forma autônoma e eficaz, especialmente em um contexto de crescente dependência de infraestruturas tecnológicas estrangeiras (Matias, 2015). A digitalização dos serviços públicos nas áreas de saúde, educação e segurança, entre outras, tem como pré-requisito o controle das infraestruturas tecnológicas, além da proteção dos dados e da privacidade dos cidadãos. No entanto, a legislação brasileira, embora tenha avançado com a promulgação de normas como a Lei Geral de Proteção de Dados Pessoais (LGPD), ainda precisa de um arcabouço regulatório e jurisprudencial robusto, bem como de políticas públicas voltadas à soberania digital.

Para fortalecer a soberania digital no Brasil, visando a efetivação de direitos sociais e a legitimação de seus processos reivindicatórios, algumas políticas públicas podem ser propostas, destacando-se tanto o que já existe na base das soluções como possíveis criações que podem preencher as lacunas existentes. Uma das principais lacunas legislativas no Brasil refere-se à ausência de uma política pública consolidada para a construção de infraestruturas digitais nacionais. Atualmente, grande parte dos serviços públicos e privados que envolvem o armazenamento e o processamento de dados brasileiros depende de plataformas tecnológicas estrangeiras, o que compromete a autonomia do país.

A Lei nº 12.965/2014, conhecida como "Marco Civil da Internet" (Brasil, 2014), estabelece princípios gerais para o uso da internet, incluindo a garantia de neutralidade da rede e a proteção à privacidade dos dados dos usuários. No entanto, a lei não prevê incentivos ou mecanismos para o desenvolvimento de infraestruturas nacionais próprias. Para preencher essa lacuna, o governo federal deve estabelecer um plano de investimento em infraestruturas digitais nacionais, incluindo a criação de servidores e data centers públicos. Esses centros de armazenamento de dados, controlados pelo Estado, poderiam garantir maior segurança e privacidade às informações pessoais dos cidadãos, especialmente no contexto de serviços públicos, como saúde (SUS) e educação (plataformas de ensino à distância). Além disso, deve-

se priorizar o desenvolvimento de softwares e plataformas tecnológicas de código aberto, com incentivo a parcerias entre instituições de pesquisa e empresas de tecnologia nacionais. Muito embora o Marco Civil estabeleça alguns princípios fundamentais, ele não se aprofunda no desenvolvimento de tecnologias nacionais. Uma possível solução seria complementar essa legislação com a criação de um programa nacional de soberania digital, formado por incentivos fiscais e tecnológicos para empresas que invistam em soluções de infraestrutura digital local.

A regulamentação de data centers no Brasil, hoje feita de forma genérica por legislações de telecomunicações, como a Lei nº 9.472, de 16 de julho de 1997, que "dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais", bem como a atuação da Secretaria de Comunicação Social do Governo Federal brasileiro (2023), deveriam ser ampliadas com normas específicas para incentivar a criação e operação de servidores locais, garantindo que dados sensíveis permaneçam no país.

Outro marco regulatório importante é a Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018 (Brasil, 2018). Tal normativa representou um avanço significativo ao regulamentar o tratamento de dados pessoais no Brasil, estabelecendo direitos e deveres para pessoas naturais e jurídicas, além de prever sanções para o descumprimento das normas. No entanto, a LGPD ainda precisa ser aperfeiçoada para garantir que o controle de dados seja, de fato, exercido no território brasileiro.

A lei não aborda explicitamente questões como a localização dos servidores e a soberania sobre os dados, especialmente em contextos transnacionais, em que empresas estrangeiras controlam o armazenamento e o processamento dessas informações. Diante desse cenário, é importante rever e complementar a LGPD com mecanismos que obriguem as empresas que atuam no Brasil a manter dados sensíveis e estratégicos, como informações sobre saúde, educação e segurança em servidores localizados no território nacional. Além disso, esse marco regulatório deve prever mecanismos de auditoria e fiscalização das empresas que operam com dados no país, assegurando que elas cumpram com as exigências de proteção de dados e segurança digital. A LGPD oferece a base legal para a proteção de dados pessoais, mas não trata diretamente da questão da soberania digital e da localização de dados. Um novo marco regulatório que estabeleça a obrigatoriedade de servidores locais seria crucial para proteger dados estratégicos e evitar que empresas internacionais tenham controle excessivo sobre informações essenciais dos cidadãos brasileiros. Essa regulamentação também deve prever mecanismos de incentivo à criação de empresas de tecnologia nacionais que forneçam serviços de armazenamento e processamento de

dados (Cueva, 2016).

Outra estratégia importante para promover e fortalecer o controle e a soberania digital e a efetivação de direitos sociais no Brasil é a criação de acordos internacionais regionais, especialmente entre países da América Latina e com os BRICS, que compartilham desafios comuns em termos de controle tecnológico. A formação de blocos regionais para o desenvolvimento de tecnologias digitais autônomas pode ser uma solução para reduzir a dependência de corporações estrangeiras, fortalecendo o controle sobre as infraestruturas digitais. No que tange à América Latina, o Brasil deve liderar iniciativas de cooperação tecnológica, promovendo a criação de tratados internacionais que tenham como objetivo o desenvolvimento conjunto de tecnologias de infraestrutura digital, incluindo servidores, redes e plataformas de dados, com controle regional. Além disso, por intermédio desses acordos, poderiam ser estabelecidos padrões regulatórios comuns para a proteção de dados e a soberania digital, garantindo que os países latino americanos detenham um controle mais eficaz sobre as informações de seus cidadãos e sobre as tecnologias usadas em seus territórios, como já ocorre na União Europeia, por meio do Conselho da Europa em sua "Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal".

Ainda que o Brasil faça parte de blocos regionais como o Mercosul, não existem iniciativas consolidadas de cooperação tecnológica voltadas à soberania digital. Essa iniciativa de estabelecer acordos internacionais pode preencher essa lacuna, promovendo o desenvolvimento conjunto de infraestruturas e regulamentos que fortaleçam a independência digital da região, além de poder gerar benefícios econômicos, criando um mercado digital integrado entre os países latino-americanos.

Esta medida é uma forma de combater uma vez mais o colonialismo em sua versão "colonização de dados", pois, parecido com o colonialismo tradicional, tem-se uma nova forma de controle e exploração onde recursos e poder são extraídos de indivíduos e comunidades. Considerando que os dados são utilizados para manipular preferências, influenciar decisões e, em última instância, gerar lucro para corporações, é necessário decolonizar, estabelecer medidas que garantam ainda mais a privacidade, autonomia e relacionamentos sociais como forma de combater a erosão da agência individual e o potencial para manipulação social e política. (Couldry; Mejías, 2019).

Por fim, há que se tratar da implementação de soluções tecnológicas nos processos reivindicatórios de Direitos Sociais. A digitalização dos serviços públicos no Brasil tem o potencial de expandir o acesso aos direitos sociais, mas a falta de controle sobre as plataformas

utilizadas e a marginalização digital representam desafios significativos (Barroso, 2024). Políticas públicas que incentivem o uso de tecnologias desenvolvidas nacionalmente ou em parceria com países da região podem garantir que os serviços de saúde, educação e segurança sejam prestados de maneira mais eficiente e equitativa, sem a interferência de empresas internacionais.

Para tanto, o governo brasileiro deve priorizar a criação de plataformas tecnológicas públicas para a prestação de serviços básicos, como saúde e educação, com infraestrutura e dados controlados pelo Estado. Programas que envolvessem a criação de plataformas nacionais de saúde e educação digitais, oferecendo serviços de telemedicina, gestão de cadastros médicos, ensino à distância e outras soluções tecnológicas, com ênfase na segurança dos dados e na inclusão digital, poderiam representar avanços significativos em prol da soberania digital. Apesar de algumas iniciativas, o Brasil não possui programas estruturados de desenvolvimento de plataformas digitais públicas. Para superar essa lacuna, é necessário implementar políticas de investimento em tecnologia nacional, incentivando startups e empresas de tecnologia brasileiras a desenvolver soluções voltadas aos serviços públicos. Esses programas devem ser regulamentados por uma política pública de inclusão digital, que garanta acesso à internet e aos serviços digitais em regiões vulneráveis.

Assim, tem-se que essas políticas públicas visam fortalecer a soberania digital no Brasil, garantindo que o país tenha controle sobre suas infraestruturas tecnológicas e que a digitalização dos serviços públicos contribua para a efetivação de direitos sociais. Ao desenvolver tecnologias próprias e consolidar um marco regulatório solidificado, o Brasil poderá promover a justiça social em um cenário digital cada vez mais complexo.

CONCLUSÃO

A discussão sobre soberania digital e direitos sociais é fundamental para entender os desafios e oportunidades que a era digital impõe ao Brasil. Este artigo buscou evidenciar como o controle das infraestruturas digitais, atualmente dominadas por grandes empresas internacionais, impacta diretamente a autonomia do Estado brasileiro e a efetivação dos direitos sociais. A dependência tecnológica, além de comprometer a implementação de políticas públicas essenciais, perpetua desigualdades e limita o acesso a serviços fundamentais, como educação, saúde e segurança.

Diante da crescente dependência de infraestruturas digitais estrangeiras, é urgente que o

Brasil adote medidas afirmativas para fortalecer sua soberania digital. A construção de infraestruturas próprias, como data centers nacionais e plataformas de código aberto, é uma necessidade premente para assegurar que o controle sobre os dados e a tecnologia se mantenha sob a jurisdição brasileira. Investir em pesquisa e desenvolvimento de tecnologias locais é fundamental para reduzir a dependência de soluções estrangeiras e garantir a autonomia do Estado em questões digitais (Marques, 2020).

A criação de um marco regulatório mais robusto também é uma medida crucial. Embora o Brasil tenha avançado com a Lei Geral de Proteção de Dados (LGPD), ainda há lacunas na regulamentação que permitem que empresas estrangeiras mantenham controle sobre dados brasileiros. Uma revisão da legislação, prevendo a obrigatoriedade de servidores locais e uma política de incentivo à criação de infraestruturas nacionais, é essencial para promover a soberania digital no país (Cueva, 2016).

Além disso, parcerias internacionais regionais, especialmente com os BRICS e outros países da América Latina, podem fomentar o desenvolvimento de tecnologias digitais autônomas e a criação de uma infraestrutura regional de compartilhamento e proteção de dados. Essas medidas afirmativas garantem não apenas o fortalecimento da soberania digital, mas também a promoção da justiça social por meio da inclusão digital de populações vulneráveis (Silveira, 2024).

As reflexões apresentadas ressaltam que a soberania digital não é apenas uma questão técnica, mas um aspecto importante da luta por justiça social. O fortalecimento do controle estatal sobre as infraestruturas digitais é uma condição indispensável para que o Brasil possa desenvolver políticas públicas que atendam às necessidades de sua população de forma equitativa. Para tanto, é imperativo que o Estado brasileiro adote estratégias que promovam a construção de soluções tecnológicas próprias, que respeitem a privacidade e a segurança dos dados das pessoas naturais e jurídicas.

A efetivação dos direitos sociais em um contexto digital exige um compromisso renovado com a inclusão e a equidade. É necessário que as autoridades públicas, a sociedade civil e o setor privado trabalhem conjuntamente para desenvolver um ecossistema digital que promova a autonomia do Estado e assegure que todos os cidadãos tenham acesso igualitário às oportunidades oferecidas pela digitalização. Isso envolve não apenas a criação de infraestruturas digitais nacionais, mas também o fortalecimento e maior desenvolvimento de legislações que garantam a proteção de dados e a privacidade dos cidadãos.

A soberania digital é um fator importante para a construção de um futuro mais justo e

igualitário. A luta por justiça social no Brasil deve ser acompanhada pela busca por um controle efetivo das infraestruturas digitais, o que permitirá ao Estado atender melhor às demandas de sua população e garantir que os processos reivindicatórios de direitos sociais sejam efetivamente respeitados e promovidos. Somente assim será possível transformar a digitalização em uma ferramenta de inclusão e justiça social, contribuindo para o desenvolvimento de um Brasil mais soberano e justo.

REFERÊNCIAS

ANTUNES, L. D. et al. *Jurisdição e conflitos de lei na era digital*: quadro político-normativo de regulação na internet. Instituto de Referência em Internet e Sociedade: Belo Horizonte, 2017. Disponível em: <http://bit.ly/2DUZ2zz>. Acesso em: 01 Set. 2024.

BARROSO, Luís Roberto. *Inteligência artificial, plataformas digitais e democracia*: Direito e tecnologia no mundo atual. Belo Horizonte: Fórum, 2024.

BELLI, Luca et al. *Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano*. Rio de Janeiro: FGV Direito Rio, 2023. Disponível em: <https://cyberbrics.info/ciberseguranca-uma-visao-sistemica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/>. Acesso em: 05 Set. 2024.

BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento*. São Paulo: Forense, 2018.

BRASIL. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 20 Set. 2024.

BRASIL. *Lei n.º 13.709, de 14 de agosto de 2018*. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, p. 59, 15 ago. 2018b. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 20 Set. 2024.

BRASIL. *Lei n.º 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 20 Set. 2024.

BRASIL. *Lei n.º 9.472, de 16 de julho de 1997*. Dispõe sobre a organização dos serviços de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais. Diário Oficial da União, Brasília, DF, 17 jul. 1997. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l9472.htm. Acesso em: 20 Set. 2024.

CINTRA et. All. *Plataformização, inteligência artificial e soberania de dados: tecnologia no Brasil 2020-2030*, 2023. Disponível em: <https://portolivres.fiocruz.br/plataformizacao-inteligencia-artificial-e-soberania-de-dados-tecnologia-no-brasil-2020-2030>. Acesso em: 15 Set. 2024.

CONSELHO DA EUROPA. *Convenção 108 +. Convenção para a proteção das pessoas relativamente ao tratamento de dados de carácter pessoal*. Disponível em: <https://rm.coe.int/cm-convention-108-portuguese-version-2756-1476-7367-1/1680aa72a2>. Acesso em: 14 Set. 2024.

COSTA, F. R. *A relativização da soberania no direito internacional público*. Tese (doutorado) – Faculdade de Direito da Universidade de São Paulo - USP. Departamento de direito

internacional e comparado: São Paulo, 2020. Disponível em <
https://www.teses.usp.br/teses/disponiveis/2/2135/tde-22032021-173031/publico/5183838_Tese_Corrigida.pdf > Acesso em: 18 Set. 2024.

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

CUEVA, Ricardo Villas Boas. A Insuficiente Proteção de Dados Pessoais no Brasil. Rio de Janeiro: *Revista Justiça e Cidadania*, nov. 2016. Disponível em:
https://www.editorajc.com.br/wp-content/uploads/2016/12/RJC-195_.pdf. Acesso em: 05 Set. 2024.

DONEDA, Danilo. A Proteção Dos Dados Pessoais como um Direito Fundamental. Rio de Janeiro. *Revista Espaço Jurídico Journal of Law [EJLL]*, v. 12, n. 2, 2011. Disponível em:
<https://portalperiodicos.unoesc.edu.br/espacojuridico/article/view/1315/658>. Acesso em: 08 Set. 2024.

DONEDA, Danilo. *Da Privacidade a Proteção de Dados Pessoais*. Revista dos Tribunais. 2. ed. 2020.

ESTADOS UNIDOS DA AMÉRICA. *Lei de Privacidade de 1974*. Estabelece um código de práticas justas de informações que regula a coleta, manutenção, uso e divulgação de informações sobre indivíduos mantidas em sistemas de registros por agências federais. Disponível em: <https://www.justice.gov/opcl/privacy-act-1974>. Acesso em: 21 Set. 2024.

KOERNER, Andrei. Capitalismo e vigilância digital na sociedade democrática. *Revista Brasileira de Ciências Sociais*, v. 36, n. 105, p. 1-6, 2021. Disponível em:
<https://www.scielo.br/j/rbcsoc/a/3RSTj7mCYh6YcHRnM8QZcYD/?format=pdf&lang=pt>. Acesso em: 14 Set. 2024.

KONIG, R. B; MÜLLER, F. R. Governança na proteção de dados e na sociedade internacional: uma análise jurídica (brasil, união europeia e estados unidos da américa). Direito, governança e novas tecnologias III [Recurso eletrônico on-line] organização CONPEDI. Coordenadores: Flavia Piva Almeida Leite; Jéssica Amanda Fachin; Jonathan Barros Vita; Valter Moura do Carmo – Florianópolis: CONPEDI, 2024. Disponível em <
<http://site.conpedi.org.br/publicacoes/v38r977z/tb6u8al5/dYsv67EwkjODHm4C.pdf> > Acesso em: 04 Set. 2024.

LEMOS, R. *Soberania digital*. Artigo publicado em 15 jan. 2015. Disponível em <
https://www.observatoriodaimprensa.com.br/e-noticias/_ed834_soberania_digital/> Acesso em: 16 Set. 2024.

MARQUES, F. M. *Regulação do fluxo de dados pessoais, entre fronteiras: os contornos e limites da decisão de adequação de países terceiros*. Dissertação (mestrado em direito). Fundação Getúlio Vargas. Escola de Direito de São Paulo, 2020. Disponível em <
<https://repositorio.fgv.br/server/api/core/bitstreams/8ae2fa18-6855-4439-8c1a-98ec42acfc4/content> > Acesso em: 09 Set. 2024.

OLIVEIRA, Luiz Fernando. *O direito ao esquecimento na história do tempo presente: o ofício*

do historiador face aos limites judiciais da memória. Tese de doutorado. Universidade Federal de Goiás. Goiânia, 2018. Disponível em: < https://files.cercomp.ufg.br/weby/up/113/o/TESE_-_LUIZ_FERNANDO_DE_OLIVEIRA.pdf >. Acesso em: 02 Set. 2024.

MATIAS, Eduardo Felipe Péres. *A humanidade e suas fronteiras: do Estado soberano à sociedade global*. 2. ed. São Paulo: Paz e Terra, 2015.

PELLEGRINI, Jerônimo et al. Inteligência local, soberania digital e soberania de dados. In: PENTEADO, Cláudio; PELLEGRINI, Jerônimo; SILVEIRA, Sérgio Amadeu da (org.). *Plataformização, inteligência artificial e soberania de dados: tecnologia no Brasil 2020-2030*. São Paulo: Ação Educativa, 2023. Disponível em: <https://portolivre.fiocruz.br/plataformizacao-inteligencia-artificial-e-soberania-de-dados-tecnologia-no-brasil-2020-2030>. Acesso em: 08 Set. 2024.

PINTO, Renata Avila. Digital Sovereignty or Digital Colonialism. *International Journal on Human Rights*. v. 15, n.27, p.15-28, 2018. Disponível em: <https://sur.conectas.org/en/digital-sovereignty-or-digital-colonialism/>. Acesso em: 12 Set. 2024.

POLIDO, F. B. P. Estado, soberania digital e tecnologias emergentes: interações entre direito internacional, segurança cibernética e inteligência artificial. *Revista de Ciências do Estado*, Belo Horizonte, v. 9, n. 1, p. 1–30, 2024. DOI: 10.35699/2525-8036.2024.53066. Disponível em: <https://periodicos.ufmg.br/index.php/revce/article/view/e53066>. Acesso em: 18 Set. 2024.

POLIDO, Fabrício B.P. *Direito Internacional Privado nas Fronteiras do Trabalho e Tecnologias*. 2ª ed. Rio de Janeiro: Lumen Iuris, 2021.

ROCHA, A. C. A. *Governança global e regulação: cooperação no sul global*. Artigo publicado em 07 Mar. 2024. Disponível em < <https://dpgconference.com.br/governanca-global-e-regulacao-cooperacao-no-sul-global/> > Acesso em: 09 Set. 2024.

SECRETARIA DE COMUNICAÇÃO SOCIAL. *O que é a Política Nacional de Cibersegurança, marco no combate aos crimes virtuais*. Disponível em: <https://www.gov.br/secom/pt-br/fatos/brasil-contrafake/noticias/2023/3/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais>. Acesso em: 17 Set. 2024.

SILVA, B. M. da. *Transferência internacional de dados na perspectiva da LGPD*. Artigo publicado em 5 jan. 2022. Disponível em < <https://www.lgpdbrasil.com.br/transferencia-internacional-de-dados-na-perspectiva-da-lgpd/> > Acesso em 04 Set. 2024.

SILVA, José Afonso da. *Curso de Direito Constitucional Positivo*. 25. ed. São Paulo: Editora Malheiros, 2005.

SILVEIRA, Sérgio Amadeu da; SILVA, Tarcízio. *Racismo algorítmico: Inteligência artificial e discriminação nas redes digitais*. São Paulo: Sesc, 2024.

SUPREMO TRIBUNAL FEDERAL. *ADPF 403*. Disponível em: < <https://portal.stf.jus.br/processos/detalhe.asp?incidente=4975500> >. Acesso em: 29 set. 2024.

SUPREMO TRIBUNAL FEDERAL. *Petição 12.404 Distrito Federal*. Disponível em: <

<https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2024/08/30171714/PET-12404-Assinada.pdf> >. Acesso em: 29 set. 2024.

SUPREMO TRIBUNAL FEDERAL. *Relatores de três ações pedem julgamento conjunto do STF em novembro de casos sobre Marco Civil da Internet e plataformas*. Disponível em: < <https://noticias.stf.jus.br/postsnoticias/relatores-de-tres-acoes-pedem-julgamento-conjunto-do-stf-em-novembro-de-casos-sobre-marco-civil-da-internet-e-plataformas/> >. Acesso em: 29 set. 2024.

SUPREMO TRIBUNAL FEDERAL. *STF determina suspensão do X, antigo Twitter, em todo o território nacional*. Disponível em: < STF determina suspensão do X, antigo Twitter, em todo o território nacional >. Acesso em: 29 set. 2024.

THE WHITE HOUSE WASHINGTON. *National Cybersecurity Strategy*. Washington D.C.: 2023. <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf>. Acesso em: 07 Set. 2024.

WOODS, Andrew Keane. Digital Sovereignty + Artificial Intelligence. In: CHANDER, Anupam; SUN, Haochen (eds). *Data Sovereignty: From the Digital Silk Road to the Return of the State* New York. Oxford: Oxford University Press, 2023. p.115-136. Disponível em: <https://academic.oup.com/book/55328/chapter/428796733>. Acesso em: 11 Set. 2024.

XINXCHUCHU, Gao. *Sovereignty and Cyberspace: China's Ambition to Shape Cyber Norms*. LSE Blogs, Londres, 18 de ago. 2022. Disponível em: <https://blogs.lse.ac.uk/cff/2022/08/18/sovereignty-and-cyberspace-chinas-ambition-to-shape-cyber-norms/>. Acesso em: 11 Set. 2024.

ZUBOFF, Shoshana. *A Era do Capitalismo de Vigilância: A luta por um futuro humano na nova fronteira do poder*. São Paulo: Intrínseca, 2021.