

**XIV ENCONTRO INTERNACIONAL
DO CONPEDI BARCELOS -
PORTUGAL**

**DIREITO, ECONOMIA E DESENVOLVIMENTO
ECONÔMICO**

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria - CONPEDI

Presidente - Profa. Dra. Samyra Haydêe Dal Farra Napolini - FMU - São Paulo

Diretor Executivo - Prof. Dr. Orides Mezzaroba - UFSC - Santa Catarina

Vice-presidente Norte - Prof. Dr. Jean Carlos Dias - Cesupa - Pará

Vice-presidente Centro-Oeste - Prof. Dr. José Querino Tavares Neto - UFG - Goiás

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos - Rio Grande do Sul

Vice-presidente Sudeste - Profa. Dra. Rosângela Lunardelli Cavallazzi - UFRJ/PUCRio - Rio de Janeiro

Vice-presidente Nordeste - Prof. Dr. Raymundo Juliano Feitosa - UNICAP - Pernambuco

Representante Discente: Prof. Dr. Abner da Silva Jaques - UPM/UNIGRAN - Mato Grosso do Sul

Conselho Fiscal:

Prof. Dr. José Filomeno de Moraes Filho - UFMA - Maranhão

Prof. Dr. Caio Augusto Souza Lara - SKEMA/ESDHC/UFMG - Minas Gerais

Prof. Dr. Valter Moura do Carmo - UFERSA - Rio Grande do Norte

Prof. Dr. Fernando Passos - UNIARA - São Paulo

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP - São Paulo

Secretarias

Relações Institucionais:

Prof. Dra. Claudia Maria Barbosa - PUCPR - Paraná

Prof. Dr. Heron José de Santana Gordilho - UFBA - Bahia

Profa. Dra. Daniela Marques de Moraes - UNB - Distrito Federal

Comunicação:

Prof. Dr. Robison Tramontina - UNOESC - Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali - Rio Grande do Sul

Prof. Dr. Lucas Gonçalves da Silva - UFS - Sergipe

Relações Internacionais para o Continente Americano:

Prof. Dr. Jerônimo Siqueira Tybusch - UFSM - Rio Grande do Sul

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA - Maranhão

Prof. Dr. Felipe Chiarello de Souza Pinto - UPM - São Paulo

Relações Internacionais para os demais Continentes:

Profa. Dra. Gina Vidal Marcilio Pompeu - UNIFOR - Ceará

Profa. Dra. Sandra Regina Martini - UNIRITTER / UFRGS - Rio Grande do Sul

Profa. Dra. Maria Claudia da Silva Antunes de Souza - UNIVALI - Santa Catarina

Educação Jurídica

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba - PR

Prof. Dr. Rubens Beçak - USP - SP

Profa. Dra. Livia Gaigher Bosio Campello - UFMS - MS

Eventos:

Prof. Dr. Yuri Nathan da Costa Lannes - FDF - São Paulo

Profa. Dra. Norma Sueli Padilha - UFSC - Santa Catarina

Prof. Dr. Juraci Mourão Lopes Filho - UNICHRISTUS - Ceará

Comissão Especial

Prof. Dr. João Marcelo de Lima Assafim - UFRJ - RJ

Profa. Dra. Maria Creusa De Araújo Borges - UFPB - PB

Prof. Dr. Antônio Carlos Diniz Murta - Fumec - MG

Prof. Dr. Rogério Borba - UNIFACVEST - SC

D597

Direito, economia e desenvolvimento econômico [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Cláudio Miguel de Sousa Cardoso; Jonathan Barros Vita; Liton Lanes Pilau Sobrinho. – Barcelos, CONPEDI, 2025.

Inclui bibliografia

ISBN: 978-65-5274-214-8

Modo de acesso: www.conpedi.org.br em publicações

Tema: Direito 3D Law

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Internacionais. 2. Direito e economia. 3. Desenvolvimento econômico. XIV Encontro Internacional do CONPEDI (3; 2025; Barcelos, Portugal).

CDU: 34



XIV ENCONTRO INTERNACIONAL DO CONPEDI BARCELOS - PORTUGAL

DIREITO, ECONOMIA E DESENVOLVIMENTO ECONÔMICO

Apresentação

O XIV Encontro Internacional do CONPEDI foi realizado entre os dias 10, 11 e 12 de setembro na cidade de Barcelos, Portugal e teve como temática central “Direito 3D Law”, sendo realizado em parceria com a Escola Superior de Gestão do Instituto Politécnico do Cávado e do Ave (IPCA).

No plano das diversas atividades acadêmicas ocorridas neste encontro, destacam-se, além das palestras e oficinas, os grupos de trabalho temáticos, os quais representam um locus de interação entre pesquisadores que apresentam as suas pesquisas temáticas, seguindo-se de debates.

Especificamente, para operacionalizar tal modelo, os coordenadores dos GTs são os responsáveis pela organização dos trabalhos em blocos temáticos, dando coerência à produção e estabelecendo um fio condutor para organizar os debates em subtemas.

No caso concreto, assim aconteceu com o GT Direito, Economia e Desenvolvimento Econômico I, o qual ocorreu no dia 11 de setembro de 2025 das 14h00 às 17h30 e foi coordenado pelos professores Jonathan Barros Vita, Liton Lanes Pilau Sobrinho e Claudio Cardoso.

O referido GT foi palco de profícuas discussões decorrentes dos trabalhos apresentados, os quais são publicados na presente obra, a qual foi organizada seguindo alguns blocos temáticos específicos, que compreenderam os 12 artigos submetidos ao GT, cujos temas são

Bloco 02 – Novas tecnologias

3. O paradoxo da inovação regulada: como o fomento ao PD&I no setor elétrico se insere na acumulação por despossessão
4. Inovação, direito e IA: observações de conceitos schumpeterianos e suas convergências jurídicas
5. Dados, soberania digital e comércio internacional: as diferentes estratégias regulatórias de União Europeia, Brasil e Estados Unidos
6. Tokenização e cadeias produtivas: inovação, governança e desenvolvimento sustentável no agronegócio

Bloco 03 – Teoria geral do direito

7. Equilíbrio entre liberdade econômica e regulação: um novo paradigma da economia brasileira
8. Dos utópicos do século XIX à economia de comunhão no século XXI: UM Estudo de caso sobre transformação econômica e social através do modelo cooperativo na região sul da Amazônia
9. A relação entre direito e estado em Weber e Kelsen

Bloco 04 – Privatizações e regulação setorial

10. Governança em políticas municipais de energia solar fotovoltaica: desafios regulatórios para parcerias público-privadas

Tendo como pano de fundo os supracitados artigos, a teoria e a prática se encontram nas diversas dimensões do direito tributário e financeiro, perfazendo uma publicação que se imagina que será de grande valia, dada a qualidade dos artigos e da profundidade das pesquisas apresentadas por diversos e eminentes pesquisadores dos mais variados estados e instituições brasileiras.

Esse é o contexto que permite a promoção e o incentivo da cultura jurídica no Brasil, consolidando o CONPEDI, cada vez mais, como um importante espaço para discussão e apresentação das pesquisas desenvolvidas nos ambientes acadêmicos da graduação e pós-graduação em direito.

Finalmente, deixa-se um desejo de uma boa leitura, fruto da contribuição de um Grupo de trabalho que reuniu diversos textos e autores de todo o Brasil para servir como resultado de pesquisas científicas realizadas no âmbito dos cursos de Pós-Graduação Stricto Sensu de nosso país, representando o Brasil no exterior com fundamental importância.

Prof. Dr. Jonathan Barros Vita – Unimar

Prof. Dr. Liton Lanes Pilau Sobrinho – Universidade do Vale do Itajaí

Prof. Dr. Claudio Cardoso - Instituto Politécnico do Cávado e do Ave (IPCA)

**DADOS, SOBERANIA DIGITAL E COMÉRCIO INTERNACIONAL: AS
DIFERENTES ESTRATÉGIAS REGULATÓRIAS DE UNIÃO EUROPEIA, BRASIL
E ESTADOS UNIDOS**

**DATA, DIGITAL SOVEREIGNTY, AND INTERNATIONAL TRADE: THE
DIFFERENT REGULATORY STRATEGIES OF THE EUROPEAN UNION,
BRAZIL, AND THE UNITED STATES**

Maria Cristina Gomes da Silva D'ornellas ¹

João Antônio de Menezes Perobelli ²

Cláudia Ernst ³

Resumo

A economia digital consolidou os dados como ativos estratégicos, essenciais para o desenvolvimento econômico, a competitividade e a inovação. Nesse cenário, os fluxos transfronteiriços de dados assumem papel central e indispensável para a dinâmica do comércio internacional contemporâneo. Entretanto, a circulação global de dados não ocorre de forma neutra, refletindo e, ao mesmo tempo, intensificando assimetrias econômicas, tecnológicas e geopolíticas. A crescente preocupação com soberania digital, segurança nacional e proteção de dados tem levado os estados a adotarem diferentes estratégias regulatórias, que revelam uma combinação complexa de interesses econômicos, jurídicos e políticos. A análise desenvolvida discute a possibilidade de construção de um regime regulatório capaz de equilibrar, de forma eficiente, os benefícios econômicos do livre fluxo de dados com a necessidade de proteger interesses estratégicos, direitos fundamentais e a autonomia tecnológica dos Estados. O trabalho evidencia que temas como localização de dados, soberania digital e regulação dos fluxos internacionais extrapolam o campo jurídico, assumindo contornos de disputas geopolíticas e econômicas que configuram as novas dinâmicas do poder no século XXI. A metodologia adotada é qualitativa e exploratória, com análise documental, normativa e bibliográfica, combinada a uma perspectiva comparada, que permite refletir sobre os desafios, as oportunidades e as contradições que caracterizam a governança dos dados na economia global.

Abstract/Resumen/Résumé

The digital economy has consolidated data as strategic assets, essential for economic development, competitiveness, and innovation. In this context, cross-border data flows play a central and indispensable role in the dynamics of contemporary international trade. However, the global circulation of data does not occur in a neutral manner; rather, it reflects and simultaneously exacerbates economic, technological, and geopolitical asymmetries. Growing concerns over digital sovereignty, national security, and data protection have led states to adopt different regulatory strategies, which reveal a complex combination of economic, legal, and political interests. This analysis explores the possibility of building a regulatory framework capable of efficiently balancing the economic benefits of free data flows with the need to safeguard strategic interests, fundamental rights, and the technological autonomy of states. The study highlights that issues such as data localization, digital sovereignty, and the regulation of international data flows go beyond purely legal considerations, taking on the contours of geopolitical and economic disputes that shape the new dynamics of power in the twenty-first century. The methodology adopted is qualitative and exploratory, based on documentary, normative, and bibliographic analysis, combined with a comparative perspective that enables a reflection on the challenges, opportunities, and contradictions that characterize data governance in the global economy.

Keywords/Palabras-claves/Mots-clés: Digital economy, International transfer of data, Digital sovereignty, International trade, Regulatory strategies

1. Introdução

A economia digital tem transformado as relações entre os estados, colocando o fluxo transfronteiriço de dados no centro das relações econômicas, sociais e políticas do século XXI. Dados se tornaram, ao mesmo tempo, um ativo estratégico, um fator de produção essencial e um elemento crítico para o desenvolvimento econômico, a inovação tecnológica e a competitividade internacional. Plataformas digitais, cadeias globais de valor e modelos de negócio baseados em inteligência artificial, computação em nuvem e internet das coisas são alguns dos exemplos mais expressivos de como a circulação de dados opera como infraestrutura invisível, porém indispensável, para o funcionamento da economia global contemporânea.

Se, por um lado, a fluidez dos dados viabiliza ganhos de eficiência, redução de custos, inovação e expansão de mercados, por outro, esse mesmo fenômeno suscita desafios jurídicos, econômicos e geopolíticos de grande magnitude. A crescente preocupação com a soberania digital, a segurança nacional, a proteção de dados pessoais e a governança econômica dos dados tem levado os Estados a desenvolverem diferentes estratégias regulatórias. Afinal, não há como deixar de observar que a circulação de dados não ocorre de forma neutra, pois pode tanto refletir quanto intensificar assimetrias econômicas, tecnológicas e geopolíticas.

Nesse contexto, observa-se uma heterogeneidade regulatória no cenário internacional, para se concluir que as escolhas normativas realizadas por cada país ou bloco econômico revelam uma combinação complexa de interesses. Entre eles estão a proteção dos titulares de dados – privacidade, a segurança nacional, o fortalecimento da competitividade econômica, a preservação da soberania digital e a busca por maior autonomia tecnológica.

Diante desse cenário, este trabalho tem como objetivo central analisar as diferentes estratégias regulatórias adotadas no âmbito da transferência internacional de dados, com foco específico nos modelos da União Europeia, do Brasil e dos Estados Unidos. A análise busca abordar – ainda que brevemente – como essas escolhas refletem a intersecção de interesses econômicos, jurídicos e geopolíticos, bem como os efeitos dessas decisões para a governança global dos dados e para o comércio internacional.

Do ponto de vista metodológico, o estudo adota uma abordagem qualitativa e exploratória, baseada na análise documental, normativa e bibliográfica, com o exame de legislação nacional e internacional, de documentos institucionais, relatórios de

organizações internacionais (como OCDE e UNCTAD) e da literatura especializada nas áreas de direito digital, direito internacional, comércio internacional e regulação econômica. A análise também incorpora uma perspectiva comparada, que permite observar as convergências e divergências entre os modelos adotados, especialmente no que se refere à articulação entre proteção de dados, soberania digital e interesses econômicos.

2. Transformação Digital e Centralidade dos Dados na Economia Global

A transformação digital de processos econômicos, comerciais e sociais, se intensifica continuamente, impulsionada pelo avanço das próprias tecnologias digitais e, principalmente, por um contexto em que a interconectividade global tem se expandido, sobretudo em razão do fluxo transfronteiriço de dados.

O fluxo transfronteiriço de dados pode ser definido como a circulação de dados pela internet, entre servidores situados em diferentes localidades geográficas, sem considerar limites territoriais. (MITCHELL & MISHRA, 2024, p. 846) Para Porger e Enders, os dados que atravessam as fronteiras nacionais podem ser divididos em três categorias distintas: (1). dados informacionais e empresariais, utilizados para dar suporte à produção, ao marketing, às vendas, aos serviços pós-venda e à funcionalidade dos produtos – categoria que também inclui dados pessoais; (2). a exportação e importação de produtos e serviços viabilizados digitalmente, bem como produtos adquiridos por meio de plataformas digitais e (3). a exportação e importação de conteúdos digitalizados, como, por exemplo, softwares, músicas e conteúdos audiovisuais. (2016, p. 01) O elemento que une todas essas atividades é a transferência de informações digitais, em formato legível por máquina, por meio da infraestrutura da internet. (LATEEF, 2025, p. 877)

A internet¹, portanto, gerou uma revolução global ao conectar pessoas, reduzir distâncias e viabilizar novas formas de interação, especialmente na esfera comercial. Na

¹ Burri observa que a internet pode ser compreendida como uma tecnologia de uso geral (General Purpose Technology – GPT), na medida em que reúne as três características que, segundo especialistas em tecnologia, definem esse tipo de inovação: (a). é amplamente utilizada; (b). possui múltiplas aplicações e (c). gera diversos efeitos indiretos e disseminados em outros setores da economia. Esta também se enquadra como uma tecnologia habilitadora, pois não oferece soluções finais, mas cria condições para o surgimento de novos modelos de negócios e processos produtivos. Nesse sentido, a autora salienta que a internet introduziu novas formas de produzir, distribuir, acessar e reutilizar informações, o que viabilizou inovações significativas – desde transformações em mercados tradicionais, como o comércio eletrônico, até a emergência de cadeias globais de valor, plataformas digitais disruptivas, redes sociais, ou ainda, aplicativos baseados na economia compartilhada, como o Uber e o Airbnb. Ver: BURRI, Mira. The impact of Digitalization on Global Trade Law. *German Law Journal*, v. 24, n. 3, 2023, pp. 551 – 573. Disponível

verdade, o crescente processo de digitalização promoveu o surgimento de diferentes estruturas que passaram a compor a nova economia digital, tais como a computação em nuvem, a inteligência artificial, o blockchain, a IoT (internet das coisas) e as plataformas. Estas últimas, em especial, merecem destaque porque não se restringem a uma aplicação específica. Ao contrário, as plataformas estão presentes/inseridas em praticamente todos os setores econômicos e sociais e, representam, de forma concreta, a lógica da monetização de dados². No contexto da prestação de serviços, Manyika *et al.* apontam exemplos de diferentes plataformas digitais amplamente utilizadas em diferentes setores em âmbito internacional/, como: eBay e Amazon, que se destacam nos mercados eletrônicos; Android e iOS, entre os sistemas operacionais; Facebook, Twitter e Instagram, nas redes sociais e YouTube, Netflix e Spotify, nas plataformas de mídia digital. Os autores também referem as plataformas que permitem o contato imediato entre empregadores e candidatos a empregos, como o LinkedIn e, ainda, entre viajantes e ofertas de hospedagem, como o Airbnb. (MANYIKA et al., 2016 *apud* WILLEMYNS, 2021, p. 09)

Cabe salientar que essas empresas não apenas operam na oferta de produtos e serviços digitais, mas também desempenham um papel estratégico muito amplo, tanto na esfera econômica quanto na geopolítica. Elas são vistas, portanto, como ferramentas de destaque e projeção de poder econômico e tecnológico, na medida em que expandem a sua atuação internacionalmente, investindo de forma intensiva em elos da Cadeia Global de Valor (General Value Chains – GVC) na economia de dados. (UNCTAD, 2021, p. 03) Esses investimentos não se limitam à coleta de dados, abrangendo também a infraestrutura crítica de transmissão – como cabos submarinos e satélites – e o armazenamento e data centers.

Nesse contexto, cabe mencionar a explicação apresentada por Willemyns, quando afirma que o comércio do século XXI é caracterizado por dois desenvolvimentos principais: o primeiro deles, refere-se à fragmentação da produção em Cadeias Globais de Valor (General Value Chains – GVC), que atravessam diversas fronteiras, ao envolver

em: <https://www.cambridge.org/core/journals/german-law-journal/article/impact-of-digitalization-on-global-trade-law/68D70BB2E3732CA766D71D81CFACC319>. Acesso em: 18/06/2025.

² É importante destacar que se reconhece, por exemplo, que as plataformas exercem influência que transcende a esfera econômico-comercial, refletindo-se também no campo político, na medida em que podem controlar o fluxo de informações, impactar na formação da opinião pública, estruturar a organização de movimentos sociais, etc. Entretanto, o foco deste estudo consiste em abordar situações relacionadas ao fenômeno da transformação digital que envolvam, diretamente, a exploração econômica de dados, no âmbito comercial.

processos produtivos cujas etapas são distribuídas entre diferentes países; o segundo, trata justamente da digitalização da produção e do comércio, que resultou, por exemplo, na intensificação do comércio transfronteiriço de produtos e serviços digitais.(2021, p. 05) Ou seja, muitas empresas utilizam ferramentas digitais em vários de seus processos e recorrerem ao fluxo transfronteiriço de dados, com o objetivo de aumentar a eficiência operacional, reduzir custos, expandir mercados, melhorar a competitividade e impulsionar/fortalecer seus modelos de negócios.

Os benefícios dos fluxos transfronteiriços de dados, no entanto, são desigualmente distribuídos entre os países, na medida em que são as economias desenvolvidas as mais favorecidas. São estas as que contam com infraestrutura digital avançada, setores tecnológicos consolidados e expressivo poder de mercado na esfera digital. (LATEEF, 2025, p. 878) Aliás, muitas big techs são consideradas ativos estratégicos no âmbito da soberania digital dos estados em que estão sediadas, visto que exercem controle sobre fluxo massivo de dados e operam em infraestruturas essenciais para a dinâmica econômica, social e até mesmo para a segurança nacional. (UNCTAD, 2021) Assim, a sua atuação transcende a lógica comercial e o âmbito especificamente econômico, para contribuir em um processo em que os estados também tratam de firmar a sua soberania no ambiente digital.

No que tange à soberania, encontram-se inseridas as questões relativas à dependência e ao colonialismo digital – ou, conforme conceito apresentado por Kwet, no uso da tecnologia digital para a dominação política, econômica e social de outra nação ou território³. (KWET, 2021 *apud* AVELINO, 2022, p. 105) Por um lado, o fluxo transfronteiriço de dados desempenha um papel fundamental para o funcionamento da economia digital e para a inserção e/ou integração de empresas no mercado global. Por outro, esse mesmo fenômeno também suscita relevantes preocupações no que se refere à soberania digital. Assim, é necessário reconhecer que os dados e as infraestruturas digitais deixaram de ser apenas instrumentos de dinamização econômica para se consolidarem como ativos estratégicos na geopolítica contemporânea.

³ Segundo Avelino, “o colonialismo digital exerce o seu poder através de equipamentos, sistemas e plataformas. Essa forma estrutural de poder digital concentra em um número pequeno de empresas todo o aparato necessário para a conectividade da internet do mundo, o que demonstra que a economia informacional caminha para o monopólio e o fortalecimento do imperialismo.” Ver: AVELINO, R. Colonialismo Digital: dimensões da colonialidade nas grandes plataformas. *In*: CASSINO, J. F., SOUZA, J., & SILVEIRA, S. A. da. (Orgs.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. São Paulo: Autonomia Literária. 2022.

3. Soberania Digital e Fluxos Transfronteiriços de Dados

O poder na economia digital — por meio do fortalecimento da soberania digital — é essencial para que os estados garantam sua autonomia e, conseqüentemente, possam exercer influência no cenário internacional. Na medida em que — de forma interconectada — os dados, as infraestruturas digitais e as plataformas tecnológicas se consolidam como ativos estratégicos, a capacidade de controlar esses recursos passa a ser determinante não apenas para proteger interesses econômicos e sociais, mas também para buscar evitar formas de dependência tecnológica.

Sob essa perspectiva, medidas como a imposição de restrições aos fluxos internacionais de dados e a formulação de regimes normativos voltados à soberania digital configuram-se como instrumentos relevantes para mitigar a dependência estrutural em relação às potências tecnológicas e, conseqüentemente, fortalecer sua capacidade de autodeterminação no ambiente digital.

Segundo Doshi e Delgado, o poder — nas relações entre estados — se estrutura por meio de dois pilares: autonomia e influência. A autonomia traduz na capacidade de um país adotar políticas internamente sem sofrer restrições externas, preservando ou aprimorando o seu próprio espaço político. Já a influência corresponde à capacidade de afetar o comportamento de outros países. Para que um país exerça influência, é necessário que, antes, possua autonomia.

Nesse contexto, a busca por autonomia — ainda que não acompanhada de influência — se revela uma estratégia de fortalecimento do espaço político e econômico doméstico, permitindo que países não identificados como grandes potências exerçam maior controle sobre seus dados, suas infraestruturas e, conseqüentemente, sobre seu próprio desenvolvimento digital. O objetivo, portanto, seria buscar reverter — ou, ao menos, minimizar — as desigualdades que caracterizam a ordem internacional, sobretudo no que diz respeito à economia digital e ao controle sobre os dados.

Belli, Gaspar e Jaswant distinguem os conceitos de soberania de dados e soberania digital, embora reconheçam que ambos são inter-relacionados. A soberania de dados é definida como a capacidade de compreender, não somente, como e por que os dados — sobretudo, os dados pessoais — são processados, mas também por quem. Ademais, a soberania de dados também se refere ao desenvolver capacidades próprias de processamento de dados e, sobretudo, regular efetivamente essas atividades, garantindo autodeterminação e controle. Já a soberania digital possui um escopo mais amplo, referindo-se à capacidade de um país exercer agência, poder e controle na configuração

de sua infraestrutura digital, dos dados, dos serviços e dos protocolos que sustentam o ambiente digital. Os autores ainda reiteram, que diante de um cenário de constante transformação digital, é impossível não tratar de temas correlatos como localização de dados/ restrição de transferência de dados e soberania digital.(2024)

A imposição de localização de dados pode adotar diferentes formas, que incluem a proibição total da transferência de dados para fora das fronteiras nacionais; a permissão para transferências internacionais, desde que uma cópia dos dados seja mantida localmente; a exigências de consenso dos provedores de dados antes de dados pessoais serem transferidos para o exterior; ou ainda a imposição de que empresas estrangeiras mantenham presença física no país para poder operar. (CHANDLER & LÊ, 2015, p. 680)

Em termos gerais, a localização de dados pode ser compreendida como uma tentativa de ampliar a autonomia no ambiente digital e mitigar riscos associados à transferência internacional de dados, especialmente no que diz respeito à segurança, privacidade e proteção de interesses estratégicos. Assim, ao exigir que dados sejam armazenados e processados localmente, os estados procuram reduzir a dependência de infraestruturas e empresas estrangeiras, proteger informações sensíveis e assegurar que suas próprias leis, e não legislações de outros países, sejam aplicáveis sobre esses dados.

Porém, para Chander e Lê, quando determinados países adotam a prática de impedir que os dados deixem as suas fronteiras, sob o argumento de proteger a segurança e a privacidade dessas informações, a imposição da localização de dados acaba produzindo efeitos totalmente contrários ao desejado. Na visão dos autores, mais do que comprometer a segurança e a privacidade, as medidas de localização de dados também podem impedir/limitar o desenvolvimento econômico e a inovação. Nisso, defendem que manter dados restritos em um território nacional, não evita o risco de governos estrangeiros acessarem tais dados por meio de ataques cibernéticos, mas pode impedir que empresas usem serviços de nuvem altamente seguros, com padrões de proteção superiores oferecidos por provedores globais. Ademais, a adoção de tal medida pode aumentar riscos internos de abuso estatal; fragmentar os mercados digitais globais, pois inviabiliza negócios baseados na circulação livre de informações; dificulta a integração em cadeias globais de valor; aumenta custos operacionais, visto que obrigar empresas a construir data centers locais ou manter servidores dentro de cada país, entre outros.(CHANDER & LÊ, 2015)

Cory e Dascoli observam, que as medidas de localização de dados estão se expandindo globalmente e refletem uma estratégia adotada por diversos países para

restringir fluxos internacionais de dados. Porém, esses autores também salientam que restrições como estas acabam gerando impactos econômicos negativos, como o aumento dos custos de produção, redução de produtividade e quebra no volume de comércio. Nesse sentido, referem que segundo modelos econométricos da Information Technology and Innovation Foundation (ITIF), o aumento de uma unidade no índice de restritividade de dados (*Data Restrictiveness Index — DRI*) gera, no acumulado de cinco anos, uma redução de 7% no volume de comércio, um aumento de 1,5% nos preços de bens e serviços e uma queda de 2,9% na produtividade. China, Indonésia, Rússia e África do Sul são citados pelo referido estudo, como exemplos de economias que vêm enfrentando aumento de preços, retração do comércio e perda de produtividade devido ao endurecimento dessas barreiras. (2021, p. 01) Ademais, segundo os autores, os formuladores de políticas adotam uma abordagem de ‘dupla utilização’ ao apresentarem propostas de localização de dados, com um objetivo oficial e aparentemente legítimo, como a proteção de dados pessoais ou a cibersegurança —, quando, na realidade, sua motivação principal (oculta) está relacionada ao protecionismo, à segurança nacional, ao maior controle sobre a Internet ou a uma combinação desses fatores. (2021, p. 04)

Nem sempre, preocupações relacionadas ao desenvolvimento e à cibersegurança são entendidas como legítimas e justificáveis para a adoção de medidas como a localização de dados. No âmbito do BRICS – Brasil, Rússia, Índia, China e África do Sul – inegavelmente há países que apresentam tendências autoritárias e históricos frágeis na proteção de direitos humanos. Porém, isto não deve implicar na constatação automática de que toda iniciativa ocidental é orientada por valores democráticos ou que qualquer iniciativa ocidental deve ser um experimento autocrático. (BELLI et al., 2024, p. 06)

Além disso, é fato que o fluxo transfronteiriço de dados é central para o funcionamento da economia digital contemporânea, sendo indispensáveis para atividades como computação em nuvem, serviços financeiros, comércio eletrônico, redes sociais, telecomunicações e até para setores como a agricultura inteligente. Nisso, tanto favorecem a eficiência operacional quanto impulsionam a inovação, o crescimento econômico e a oferta de serviços. Belli, Gaspar e Jaswant afirmam, inclusive, que “(u)m dos principais benefícios de viabilizar os fluxos de dados é a promoção da cooperação internacional e da prestação de serviços em nível global, permitindo organização de empresas de forma multinacional, com redução de custos, aumento de eficiência e escalabilidade.”(2024, p. 13)

Nesse sentido, é claro que se admite que a restrição do fluxo de dados traz desvantagens quando imposta arbitrariamente. Mas também é importante salientar, que em determinados casos, esta pode contribuir para a segurança, produção nacional e para o desenvolvimento tecnológico. Com a rápida evolução tecnológica, não há como ignorar que proteger nacionalmente dados considerados estratégicos e priorizar a permanência destes dentro das fronteiras de um país, pode ser uma alternativa para a garantia de que informações valiosas efetivamente contribuam para a inovação local e produção nacional.

Diante desse cenário, torna-se evidente que as escolhas regulatórias feitas pelos Estados, especialmente no campo da proteção de dados, não são neutras, tampouco motivadas por uma única lógica. Na prática, os quadros normativos refletem a intersecção de múltiplos interesses — econômicos, geopolíticos, de segurança nacional, de promoção da inovação, de proteção da privacidade e, em alguns casos, até de caráter protecionista — mas ainda assim, justificáveis.

4. Proteção de Dados e Estratégias Regulatórias

Segundo dados da UNCTAD, até maio de 2025, 155 países adotaram leis/regulamentações relativas à proteção de dados, sendo que várias estabelecem regras específicas sobre a transferência internacional de dados pessoais. Cabe observar, ainda, que muitas dessas leis que estão sendo promulgadas nos últimos anos possuem efeitos extraterritoriais, o que significa que podem incidir simultaneamente sobre uma mesma operação de tratamento de dados, independentemente do local em que ela ocorra. Podem ser aplicadas mesmo quando o tratamento dos dados ocorre fora de um território nacional, desde que envolva dados de seus residentes. São legislações que, portanto, não se limitam a regular o tratamento interno de dados, abrangendo também a sua movimentação internacional, ao impor requisitos que visam assegurar a proteção dos dados mesmo quando circulam além das fronteiras nacionais (Casalini e López González, 2019).

Além disso, essas legislações também podem prever restrições/limitações aos fluxos internacionais de dados, como, a exigência de garantias específicas para a transferência de dados, o reconhecimento de decisão de adequação ou, ainda, a obrigatoriedade de localização de dados.

As escolhas regulatórias adotadas pelos países, tanto no que se refere à aplicação extraterritorial de suas leis de proteção de dados quanto à imposição de restrições ao fluxo transfronteiriço de dados, são usualmente justificadas por diferentes fundamentos. Entre eles, destacam-se a necessidade de garantir a conformidade entre leis nacionais de

proteção de dados, a proteção da segurança nacional, a promoção do desenvolvimento econômico em âmbito doméstico e a prevenção de riscos associados a ameaças cibernéticas. (MITCHELL & MISHRA, 2024, p. 847; CHANDER & Lê, 2015, p. 679)

A União Europeia, por exemplo, prioriza em sua legislação a proteção de dados pessoais como um direito fundamental. (CUSTERS & MALGIERI, 2022) Isso explica a adoção de um modelo regulatório rigoroso, por meio do Regulamento Geral sobre Proteção de Dados (GDPR). Além de impor obrigações aos agentes estabelecidos dentro do bloco europeu, o GDPR também se aplica extraterritorialmente. Ou seja, o seu alcance também abrange empresas e organização situadas fora da União Europeia sempre que realizarem o tratamento de dados de pessoas localizadas no território europeu, seja porque oferecem produtos ou serviços a esses titulares, seja porque monitoram seu comportamento. Esse regime estabelece que a transferência de dados pessoais para países terceiros só pode ocorrer quando houver garantias de que o nível de proteção oferecido fora da União Europeia seja equivalente àquele adotado internamente. Nesse sentido, impõe os instrumentos de decisões de adequação, cláusulas contratuais padrão, entre os seus mecanismos de salvaguarda. (ROTENBERG, 2020)

A lógica em manter a sua forte posição de princípio sobre privacidade, se reflete – inclusive – nas relações com os Estados Unidos (outra grande potência), visto que ambos países enfrentaram sucessivos desafios na tentativa de facilitar o fluxo de dados entre os seus territórios. Primeiramente, tiveram o acordo *Safe Harbor* (2000 – 2015) invalidado no caso *Schrems I* e, posteriormente, o *Privacy Shield* (2016 – 2020) anulado no caso *Schrems II*. Somente recentemente, em 2023, foi adotado pelo Comissão Europeia o *Data Privacy Framework*, por meio de uma decisão de adequação que reconheceu que os Estados Unidos passaram a oferecer um nível de proteção de dados considerado “essencialmente equivalente” ao da União Europeia. (THEODORAKIS & TZEFERAKOU, 2023)

Trata-se de um cenário que demonstra que o modelo europeu efetivamente assegura elevados padrões de proteção de dados, mas também gera dificuldades operacionais, especialmente para empresas.

Com isso, existem críticas ao estabelecido pela GDPR, na medida em que os seus elevados requisitos de conformidade – embora legítimos sob a ótica da proteção de direitos fundamentais – revelam-se, em determinados contextos, barreiras ao comércio e

à livre circulação de dados. Segundo o entendido por Custers e Malgieri⁴, o GDPR, ao consolidar a proteção de dados como um direito fundamental, entra em tensão direta com práticas comerciais baseadas no comércio de dados pessoais. Isso gera barreiras não apenas ao comércio digital internacional, mas também cria desafios internos para o desenvolvimento do próprio mercado digital europeu. (2022)

Li *et al.*, no entanto, apresentam uma análise distinta dos impactos que podem ser gerados a partir de regulamentações de proteção de dados e privacidade, como o GDPR. Para os autores, o Regulamento Europeu produz efeitos ambivalentes sobre o comércio digital internacional, na medida em que pode gerar tanto impacto positivos quanto negativos. Embora as normas previstas pelo GDPR impliquem em custos de conformidade mais elevados para as empresas, quando implementadas de forma transparente, podem fortalecer a confiança dos consumidores, reduzir vieses em favor de produtos/serviços nacionais e, conseqüentemente, facilitar a entrada de empresas estrangeiras no mercado europeu. (2024)

No Brasil, houve a promulgação da Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), sancionada em 2018, com entrada em vigor em 2020. Inspirada na GDPR da União Europeia, a LGPD reflete uma lógica baseada na proteção dos direitos fundamentais. (BOTELHO, 2020) Assim, rompe com a lógica anterior de autorregulação, passando a estabelecer regras específicas para o tratamento de dados pessoais no país. Segundo Iramina, tanto a LGPD quanto a GDPR adotaram uma abordagem estratégica no tratamento de dados pessoais, estimulando que empresas incorporem boas práticas como diferencial competitivo. (2020, p. 93)

A LGPD está entre as legislações que prevê a sua abrangência extraterritorialmente, pois não se aplica exclusivamente a empresas e organizações que não estejam localizadas no Brasil, mas também àquelas estabelecidas no exterior. A aplicação do estabelecido pela LGPD depende de dois critérios: se o tratamento dos dados e a oferta de serviços e produtos resultantes desse tratamento ocorreram no

⁴ Sobre a crítica apresentada por Custers e Malgieri à mercantilização dos dados pessoais, a partir de sua natureza de direito fundamental inalienável, cabe comentar que esta encontra eco na análise feita por Sadowski, para quem os dados não devem ser compreendidos como mercadorias tradicionais, mas como uma forma de capital. Isto porque, tal perspectiva parece reforçar que, tanto sob o ângulo jurídico quanto econômico, os dados ocupam uma posição *sui generis*/peculiar: juridicamente, pela impossibilidade de alienação plena em razão da proteção fundamental conferida; economicamente, pelo fato de que os dados, longe de serem consumidos ou trocados definitivamente, alimentam processos contínuos de acumulação, controle e geração de valor no capitalismo digital. Ver: CUSTERS, B, MALGIERI, G. Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data. *Computer Law & Security Review*, 45, 2022; SADOWSKI, J. When data is capital: Datafication, accumulation, and extraction. *Big Data & Society*, January – June 2019.

território nacional, ou se a coleta dos dados pessoais foi realizada no Brasil. Na prática, essa lógica segue o modelo de proteção extraterritorial, segundo o qual os direitos dos titulares devem ser preservados, independentemente da localização dos dados.

Ademais, estabelece normas relativas à transferência internacional de dados e, de uma forma tautológica, a define como a transferência de dados pessoais a país estrangeiro ou organismo internacional do qual o Brasil seja membro. (Carvalho, 2020, p. 624; Pinho e Cavalcante, 2024, p. 204) A transferência internacional de dados esta baseada na exigência de garantias de proteção compatíveis com a legislação nacional. Isso significa que a realização dessa transferência não pode ocorrer de maneira livre ou irrestrita, sendo condicionada à demonstração de garantias que resguardecem os direitos dos titulares.

Para viabilizar essa proteção, a regulamentação brasileira adota mecanismos semelhantes ao da GDPR europeia. O primeiro deles se refere à avaliação de adequação, na qual a autoridade nacional pode reconhecer que determinado país ou organismo internacional oferece um nível de proteção de dados compatível com o brasileiro. A tarefa de estabelecer esses parâmetros recai sobre a Nacional de Proteção de Dados (ANPD)⁵, que detém competência para avaliar os elementos normativos, institucionais e práticos do país ou organismo objeto da análise. Contudo, essa hipótese, embora formalmente prevista, é reconhecida como uma das mais complexas, justamente porque quando foi estabelecida, carecia de critérios pré-definidos na legislação. Ou seja, sem parâmetros claros, tratou de gerar insegurança e dependência de soluções alternativas.

Sem a decisão de adequação, o sistema permite que a transferência ocorra mediante a adoção de instrumentos específicos que garantam a proteção dos dados. Entre eles estão as cláusulas contratuais específicas, elaboradas caso a caso, e as cláusulas-padrão, previamente aprovadas pela ANPD ou baseadas em modelos internacionais. Outra opção são as normas corporativas globais, que padronizam as práticas de proteção de dados dentro de empresas ou grupos multinacionais.

A Resolução nº 19/2024 da ANPD, aprovada recentemente, definiu regras de reconhecimento de adequação de outras jurisdições e aprovou cláusulas contratuais

⁵ Interessante observar que, embora a LGPD tenha sido aprovada em agosto de 2018, sofreu vetos por parte do então Presidente da República. Um dos vetos foi justamente o que dizia respeito à criação da ANPD, sob o argumento de que a sua instituição deveria ocorrer por ato do Executivo. Em razão disso, em dezembro de 2018, foi editada a MP 869/2018, que somente foi convertida em lei em junho de 2019, dando origem formal à ANPD. A autoridade passou a ter a incumbência de cumprir com uma série de funções, tais como: a edição de normas e a interpretação da própria LGPD. Cf. FINKELSTEIN, M. e FINKELSTEIN, C. 2019, p. 294. Ademais, vale referir que por meio da Lei n. 14.460 de 25 de outubro de 2022, a ANPD foi transformada em autarquia de natureza especial.

padrão. No entanto, a adoção desses mecanismos não elimina os desafios. O fato de ainda persistir a ausência de decisões de adequação com mercados relevantes, como os Estados Unidos, impõe custos operacionais às empresas, que precisam estruturar contratos complexos ou adotar regras internas rigorosas para assegurar a conformidade.

O Brasil não adota medidas de localização de dados na LGPD. Apenas, como já referido anteriormente, a possibilidade de ser aplicada extraterritorialmente, especialmente, nas situações em envolvam disputas internas relativas ao tratamento ou armazenamento desses dados, ou, ainda, no caso de violações à legislação brasileira de proteção de dados cometidas por atores estrangeiros. Nesse contexto, Doshi e Delgado lamentam que não tenha sido considerada a possibilidade de a legislação exigir que, ao menos, determinadas categorias de dados fossem armazenadas no próprio país. No lugar de uma indicação direta de situações em que a localização de dados seria necessária, houve a opção por se contentar com um suposto alcance extraterritorial da legislação brasileira que, na prática, não conta com qualquer efetividade em termos de *enforcement*. (2024, p. 146)

No caso dos Estados Unidos, historicamente sempre houve o posicionamento de estimular a livre circulação dos dados, tanto em âmbito nacional quanto internacional. Diferentemente da União Europeia, por meio do GDPR, e de outros países que adotam um regime baseado na proteção de dados como direito fundamental, os Estados Unidos priorizaram uma abordagem ancorada no mercado. Com isso, os dados eram tratados – unicamente – como ativos econômicos e comerciais.

É verdade que o país ainda não possui uma lei federal geral de proteção de dados, mas, recentemente⁶, houve uma alteração significativa na postura dos Estados Unidos diante do controle do fluxo internacional de dados. Assim, admitindo a possibilidade de restrição à circulação de dados centrada na lógica da segurança nacional, os Estados Unidos adotaram o *Final Rule: Provisions Pertaining to Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern*. Este somente se aplica a certos países (*countries of concern* – países de preocupação) – China (incluindo Hong Kong e Macau), Cuba, Irã, Coreia do Norte,

⁶ A *Final Rules* do *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* estão em vigor desde o dia 8 de abril de 2025. No entanto, há um período de transição que se estende até o dia 8 de julho de 2025. Durante este período o Departamento de Justiça dos Estados Unidos será mais tolerante quando às novas exigências impostas, desde que as empresas demonstrem boa-fé no processo de adaptação. Ver: **PITTMAN, F. P.; ANDERSON, H.; LIM, D. H.; WANG, Y. DOJ Issues Final Rule Prohibiting and Restricting Transfers of Bulk Sensitive Personal Data.** Insight Alert, White & Case, 27 fev. 2025.

Rússia e Venezuela e a tipos específicos de dados. Conforme o Departamento de Justiça norte-americano (DJO), “esses países de preocupação demonstram a intenção e a capacidade de usar dados relacionados ao governo dos Estados Unidos e dados pessoais sensíveis de cidadãos americanos para ameaçar a segurança nacional dos EUA, inclusive por meio da espionagem, espionagem econômica, vigilância, coerção e influência, chantagem, influência estrangeira nociva, repressão à liberdade de expressão de cidadãos norte-americanos, perseguição a jornalistas, líderes políticos, membros de comunidades marginalizadas e outros grupos, além de práticas ilícitas conduzidas por meio cibernéticos”. (DJO, 2025 *apud* PITTMAN, *et al.*, 2025)

Estes são somente alguns exemplos de que os efeitos da transformação digital não se manifestam de forma homogênea, pois atingem de maneira distinta múltiplas dimensões – econômicas, comerciais, sociais e políticas.

5. Conclusão

A análise desenvolvida permite concluir que o fluxo transfronteiriço de dados se consolidou como elemento estrutural da economia digital e do comércio internacional contemporâneo, refletindo e, ao mesmo tempo, reforçando assimetrias econômicas, tecnológicas e geopolíticas no cenário global. Embora os dados sejam fundamentais para viabilizar modelos de negócios, inovação e integração em cadeias globais de valor, sua circulação não ocorre de forma neutra. Ao contrário, ela está diretamente vinculada à afirmação de soberania digital, à proteção de interesses estratégicos e à defesa da competitividade econômica de cada país ou bloco econômico.

O exame comparado dos modelos regulatórios adotados pela União Europeia, Brasil e Estados Unidos revela estratégias normativas orientadas por distintas racionalidades. Enquanto a União Europeia mantém uma abordagem baseada na proteção de dados como direito fundamental, impondo rigorosas restrições às transferências internacionais, o Brasil optou por um modelo intermediário. A legislação brasileira adota a lógica da proteção de direitos, mas sem exigir a localização de dados, baseando-se, em grande medida, na aplicação extraterritorial da LGPD — estratégia que, na prática, revela-se limitada quanto à sua efetividade no enforcement. Já os Estados Unidos, historicamente defensores da livre circulação de dados sob uma ótica de mercado, passaram recentemente a adotar uma abordagem restritiva, ancorada em razões de segurança nacional, especialmente em relação a países classificados como “de preocupação”.

Esse cenário evidencia que as escolhas regulatórias não se pautam exclusivamente pela proteção da privacidade, mas também refletem objetivos estratégicos relacionados à segurança, autonomia tecnológica, competitividade econômica e até ao exercício de poder no ambiente digital. Constata-se, ainda, que os debates sobre localização de dados, jurisdição extraterritorial e controle dos fluxos internacionais transcendem discussões meramente técnicas, assumindo dimensão política, econômica e geopolítica de elevada relevância.

Diante da crescente interdependência digital e das assimetrias que caracterizam a economia global, a governança dos fluxos de dados se apresenta como um dos principais desafios regulatórios do século XXI. A busca por equilíbrio entre os benefícios da circulação internacional de dados e a necessidade de proteger soberania, segurança e direitos fundamentais permanece como uma questão aberta, que exigirá, cada vez mais, soluções jurídicas inovadoras, cooperação internacional e formulações regulatórias sensíveis às dinâmicas de poder e às desigualdades estruturais do sistema internacional.

Referências

- AVELINO, R. Colonialismo Digital: dimensões da colonialidade nas grandes plataformas. In: CASSINO, J. F., SOUZA, J., & SILVEIRA, S. A. da. (Orgs.). **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. São Paulo: Autonomia Literária. 2022.
- BELLI L., GASPAR, W.B., JASWANT, S. Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. **Computer Law & Security Review**. Special issue on Digital Transformation in the BRICS Countries, 2024. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364924000839> acesso em: 19 jun. 2025.
- BURRI, Mira. Data Flows and Global Trade Law: Tracing Developments in Preferential Trade Agreements. In: **Big Data and Global Trade Law**, Mira Burri (Ed.), Cambridge: Cambridge University Press, 202, pp. 11–41.
- CHANDER, A.; LÊ, P. Data Nationalism. **Emory Law Journal**, v. 64, n. 3, p. 677-739, 2015. Disponível em: <https://ssrn.com/abstract=2577947>. Acesso em: 19 jun. 2025.
- CASSINO, J. F.; SOUZA, J.; SILVEIRA, S. A. da. (Orgs.). (2022). **Colonialismo de dados: como opera a trincheira algorítmica na guerra neoliberal**. São Paulo: Autonomia Literária.

CORY, Nigel; DASCOLI, Luke. **How barriers to cross-border data flows are spreading globally, what they cost, and how to address them.** Washington, D.C.: **Information Technology and Innovation Foundation (ITIF)**, July 2021. Disponível em: <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally/>. Acesso em: 20 jun. 2025.

CUSTERS, B.; MALGIERI, G. Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data. **Computer Law & Security Review**, v. 45, 2022. p. 1 – 16. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364922000309> Acesso em: 13 jun. 2025.

DOSHI, V.; DELGADO, HE. Digital Statecraft of Middle Powers: Tech Landscape and Digital Sovereignty in Brazil and India. In: Jiang M, Belli L, eds. **Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance.** Communication, Society and Politics. Cambridge University Press; 2025:124-147. Disponível em: <https://www.cambridge.org/core/books/digital-sovereignty-in-the-brics-countries/27E9FD7E4579C76C8D4BA52F7670B431> Acesso em: 13 jun. 2025.

FINKELSTEIN, M. E.; FINKELSTEIN, C. Privacidade e lei geral de proteção de dados pessoais. **Revista de Direito Brasileira**, v. 23, n. 9, p. 284-301, 2019. Disponível em: <https://indexlaw.org/index.php/rdb/article/view/5343/4545>. Acesso em: 20 abr. 2025.

IRAMINA, A. RGPD v. LGPD: Adoção Estratégica da Abordagem Responsiva na Elaboração da Lei Geral de Proteção de Dados do Brasil e do Regulamento Geral de Proteção de Dados da União Europeia. **Revista de Direito, Estado e Telecomunicações**, Brasília, v. 12, nº 2, p. 91-117, 2020.

LI, Z.; LEE, G.; SANTANAM, R.; SHI, Z. (Michael). Impact of the GDPR on the Global Mobile App Market: Digital Trade Implications of Data Protection and Privacy Regulations. **Information Systems Research**, ahead of print, 2024. Disponível em: <https://pubsonline.informs.org/doi/epdf/10.1287/isre.2022.0421> Acesso em: 09 jun. 2025.

PITTMAN, F. P.; ANDERSON, H.; LIM, D. H.; WANG, Y. **DOJ Issues Final Rule Prohibiting and Restricting Transfers of Bulk Sensitive Personal Data.** Insight Alert, White & Case, 27 fev. 2025. Disponível em: <https://www.whitecase.com/insight-alert/doj-issues-final-rule-prohibiting-and-restricting-transfers-bulk-sensitive-personal>. Acesso em: 20 jun. 2025.

PORGES, A.; ENDERS, A. **Data Moving Across Borders: The Future of Digital Trade Policy** (E15 Initiative Think Piece). Geneva: International Centre for Trade and Sustainable Development & World Economic Forum. 2016. Disponível em: https://www.researchgate.net/publication/303062948_Data_Moving_Across_Borders_The_Future_of_Digital_Trade_Policy Acesso em: 10 jun. 2025.

ROTENBERG, J. Privacy before trade: assessing the WTO-consistency of privacy-based cross-border data flow restrictions. **University of Miami International and Comparative Law Review**, v. 28, n. 1, Fall 2020, p. 97-138.

SADOWSKI, J. When data is capital: Datafication, accumulation, and extraction. **Big Data & Society**, January – June 2019

THEODORAKIS, N. I.; TZEFERAKOU, D. The EU-US Data Privacy Framework: A new path for transatlantic data transfers? **TTLF Working Papers**, n. 109, 2023. Disponível em: <https://law.stanford.edu/publications/the-eu-us-data-privacy-framework-a-new-path-for-transatlantic-data-transfers/>. Acesso em: 10 jun. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-362/14, Maximillian Schrems v. Data Protection Commissioner. Decisão de 6 de outubro de 2015. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=E> N. Acesso em: 28 abr. 2025.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. Processo C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd e Maximillian Schrems. Decisão de 16 de julho de 2020. Disponível em: <https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&doclang=E> N. Acesso em: 28 abr. 2025.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. **Digital Economy Report 2021: Cross-border data flows and development: for whom the data flow**. 2021. Disponível em: https://unctad.org/system/files/official-document/der2021_overview_en_0.pdf. Acesso em: 16 abr. 2025.

WILLEMYNS, Ines. **Digital Services in International Trade Law**. Cambridge: Cambridge Press, 2021.