RELATÓRIO

Tratados e Acordos para Transferências Internacionais de Dados

AUTOR
PEDRO GUEIROS

EDITORAÇÃO E REVISÃO
CELINA BOTTINO
CHRISTIAN PERRONE

PROJETO GRÁFICO
MARIANA BERTOLUCI

Sumário

Resumo executivo

Não há dúvidas de que a circulação de dados exerce enorme impacto às relações e atividades humanas ao redor do mundo. Basta pensar que se você está lendo isso, nesse momento, é porque há um fluxo facilitado de informações sendo travadas na rede mundial de computadores. Mas para que essa informação, instrumentalizada por diversos atores privados, chegue de forma livre e desimpedida não é uma tarefa relativamente simples. Por mais banal que pareça, há certo privilégio para que isso aconteça de forma desembaraçada.

Ao redor do mundo, existem variadas regras, acordos e tratados que disciplinam tanto em nível nacional, como bilateral ou multilateralmente os limites e as possibilidades para que os dados pessoais fluam e percorram não apenas entre cabos físicos submarinos, que conectam os diversos continentes do globo, como também para estejam virtualmente disponíveis em nuvem.

Diferentes interpretações ou alinhamentos geram, portanto, diferentes gradações no respectivo proteção dos dados. Identificar os principais fatores que levam a tendências mais liberais ou mais restritivas é crucial para compreender qual deve ser a tônica adequada e consequentemente essencial às transferências internacionais de dados. Devem, afinal, ser particularmente delineadas num fluxo mais livre, mas com confiança.

O presente relatório está subdividido da seguinte forma:

O **capítulo 1** traz a introduz a discussão sobre tratados internacionais e o seu impacto no fluxo global de dados, além de apresentar a metodologia empregada no desenvolvimento desta pesquisa, baseada na análise e revisão sistemática de como tratados e acordos regulamentam, viabilizam ou até mesmo limitam o fluxo transfronteiriço de dados pessoais;

O **capítulo 2** trata das duas perspectivas majoritárias no âmbito das transferências internacionais de dados, quais sejam a: (i) primazia pela maior facilitação de transferências internacionais de dados pessoais e; (ii) priorização da proteção conferida aos dados pessoais. Objetiva-se, para tanto, destacar como estas visões, teoricamente antagônicas entre si, podem trazer consequências positivas e negativas ao panorama socioeconômico dos diferentes países;

O **capítulo 3** aborda os potenciais impactos ao fluxo transfronteiriço, a partir da construção e consequente imposição por ordenamentos jurídicos de mecanismos mais rígidos ou flexíveis à autorização de exportações de dados pessoais. Por meio desta análise, verifica-se os seguintes padrões: (i) restrições nacionais; (ii) restrições indiretas; (iii) acordos que visam regular obrigações de localização forçada e; (iv) acordos que apenas abordam a importância da proteção de dados pessoais e a livre circulação;

O **capítulo 4** discute as estratégias dos principais tratados e acordos internacionais, incluindo tratativas comerciais e *sandboxes* regulatórios que envolvem a transferência de dados pessoais. Analisa-se as principais características sob cinco pontos analíticos, se: (i) como regra, as transferências são autorizadas; (ii) remetem a algum padrão ou norma específica; (iii) há a criação de uma norma ou ainda se obriga à criação de regulação em nível interno; (iv) há menções à computação em nuvem e seus serviços; e (v) os documentos em si se relacionam com regulações setoriais específicas;

O **capítulo 5** sistematiza os referidos pontos analíticos, de modo a verificar como se operam na prática os tratados e acordos internacionais para fins de transferência internacional de dados;

O **capítulo 6**, por fim, apresenta os principais resultados obtidos com o estudo, traçando considerações daquilo que parece ser de maior relevância ao contexto brasileiro para fins de regulamentação das transferências internacionais de dados pessoais. Sob indispensabilidade de soluções digitais a

interesses de ordem não apenas nacional, mas efetivamente existencial, o presente relatório busca evidenciar que a regulamentação sobre as transferências internacionais está diretamente associada ao futuro do desenvolvimento socioeconômico do Brasil.

1. Introdução e metodologia

Em um planeta que se insere progressivamente na realidade hiperconectada, o dinamismo das relações humanas pressupõe comunicações cada vez mais instantâneas, ágeis e fluidas. Os benefícios obtidos através do uso de dados pessoais movimenta todo um cenário de inovação e desenvolvimento socioeconômico, tanto de iniciativas públicas quanto privadas, a exemplo das vantagens com relação ao uso de tecnologias 5G, Internet das Coisas e Inteligências Artificiais.

Para dimensionar a expressividade desse dinamismo próprio de uma *Inovação Orientada a Dados*[1], estimativas apontavam que até o final de 2022, **65% do PIB mundial** esteve atrelado à perspectiva de fluxos transfronteiriços de dados pessoais[2]. Apenas em um período de pouco mais de 10 anos a **largura de banda transfronteiriça de dados** em uso cresceu **148 vezes**[3]. Sob uma escala global, apenas em 2020, 64.2 zettabytes (ou 64,000,000,000,000 gigabytes) de dados digitais foram criados ou replicados.

Para países em desenvolvimento, como Brasil, Indonésia e África do Sul, no que concerne à sistemas movidos à Internet das Coisas (IoT na sigla inglesa), estima-se que cerca de **59% e 68% de ganhos no PIB serão diretamente atribuíveis a fluxos**

[1] Para a OCDE, uma Inovação Orientada por Dados "constitui um pilar fundamental nas fontes de crescimento do século XXI. A confluência de várias tendências, incluindo a crescente migração de atividades socioeconômicas para a Internet e o declínio no custo de coleta, armazenamento e processamento de dados, estão levando à geração e uso de grandes volumes de dados – comumente referidos como " grandes dados". Esses grandes conjuntos de dados estão se tornando um ativo essencial na economia, promovendo novos setores, processos e produtos e criando vantagens competitivas significativas". ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. Data-driven innovation for growth and well-being. Disponível em: <https://www.oecd.org/sti/ieconomy/data-driven-innovation.htm>. Acesso em: 06.06.2022.

[2] ZURICH INSURANCE. Cross-border data flows: Designing a global architecture for growth and innovation. Disponível em: <https://www.zurich.com/en/knowledge/topics/digital-data-and-cyber/cross-border-data-flows-designing-global-architecture-for-growth-and-innovation>. Acesso em: 06.09.2022.

[3] MCKINSEY GLOBAL INSTITUTE. Globalization in transition: The future of trade and value chains. Disponível em: <https://www.mckinsey.com/featured-insights/innovation-and-growth/globalization-in-transition-the-future-of-trade-and-value-chains>. Acesso em: 06.06.2022.

transfronteiriço de dados (em grande parte, pessoais)[4]. Em outras palavras, nunca foi tão necessário intermediar um volume de dados tão massivo como nos dias atuais.

Mesmo reconhecendo que cada país possui seus próprios regramentos quanto a aspectos como Internet, privacidade e proteção de dados, uma espécie de **confiança recíproca e multilateral é vital** ao atual estágio de desenvolvimento tecnológico. Chega-se ao conceito de um *Fluxo Livre de Dados com Confiança* (DFFT)[5], termo cunhado visando à construção de uma principiologia básica para a criação de regras no campo das transferências de dados entre fronteiras[6].

Ainda sob os efeitos críticos de uma pandemia global, que impôs necessárias medidas de distanciamento social, a essencialidade da digitalização de bens e serviços digitais evidenciou que a cooperação internacional é a chave para a própria continuidade da vida humana. Interesses de ordem nacional e existencial, a exemplo do tempo recorde da produção da vacina contra a covid-19, **são melhores solucionados por meio da regulação do fluxo transfronteiriço de dados pessoais**[7].

O relatório é parte de um esforço maior - são duas pesquisas paralelas - e busca apresentar as opções atualmente adotadas para regular a interface das relações comerciais e os tratados e acordos internacionais que buscam criar um marco para as transações transfronteiriças. O presente explora as as tipologias destes tratados e acordos internacionais, no tocante às respectivas diretrizes para a

[4] GLOBAL SYSTEM FOR MOBILE COMMUNICATIONS. *Cross-Border* Data Flows: The impact of data localisation on IoT. Disponível em: <https://www.gsma.com/publicpolicy/wp-content/uploads/2021/01/Cross_border_data_flows_the_impact_of_data_localisation_on_IoT_Full_Report.pdf>. Acesso em: 02.06.2022.
[5] Sigla em inglês para Data Free Flow with Trust.
[6] WORLD ECONOMIC FORUM. Every country has its own digital laws. How can we get data flowing freely between them? Disponível em: <https://www.weforum.org/agenda/2022/05/cross-border-data-regulation-dfft/>. Acesso em: 06.06.2022.
[7] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow. Nova York: United Nations Publications, 2021.

permissão ou vedação de transferências internacionais de dados pessoais entre as diferentes jurisdições, **identificando quais são as respectivas limitações e facilitações**.

Mais do que nunca, as relações de comércio internacional hoje em muito dependem da possibilidade de haver fluxos internacionais de dados, inclusive dados pessoais. O modo como estes tratados e acordos regulam essa fluidez informacional pode ter um impacto significativo não apenas no nível de interação comercial, como também na proteção dos dados para além das fronteiras geográficas.

Frente à projeção de assimetrias de interesses genuinamente relevantes ao desenvolvimento socioeconômico internacional, busca-se verificar como eventuais impasses vêm sendo dirimidos. Para tanto, torna-se relevante levar em consideração alguns eixos voltados à tutela da proteção de dados pessoais, como os direitos à privacidade, autodeterminação informativa e livre desenvolvimento da ordem econômica.

Em última análise, o propósito é propor elementos para um marco para a regulação de transferências internacionais de dados, especialmente no âmbito das atribuições da Autoridade Nacional de Proteção de Dados (ANPD). Como ilustra Stefano Rodotà, aliás, a relevância da temática está identificada na união de *condições* mínimas de tutela da privacidade ao lado de *condições* de reciprocidade[8]. Logo, "*[p]arece portanto necessária, antes do mais, uma análise mais acurada dos diversos interesses identificados sob a fórmula geral da circulação transnacional dos dados*"[9].

[8] RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Renovar: Rio de Janeiro, 2008, p. 66.
[9] Ibid.

2. Identificando as atuais perspectivas para as transferências internacionais de dados

A reflexão quanto à harmonização internacional de regras para a proteção da circulação de dados pessoais não é propriamente uma novidade. Em meio à evolução dos direitos associados à privacidade e à proteção de dados pessoais inserida no bojo de sucessivas revoluções técnico-científicas, o fluxo informacional tornou-se progressivamente mais imediato e automatizado, especialmente sob a perspectiva digital. Nesse sentido, estabelecer parâmetros de controle sobre os dados pessoais passou a estar diretamente associado à influência, reciprocidade e poder exercidos pelas Nações.

Tradicionalmente, as primeiras políticas transnacionais sobre mecanismos para transferências internacionais de dados pessoais iniciaram-se a partir de arranjos plurilaterais, a exemplo das Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais, estabelecidas pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE). À luz das clássicas regras, tem-se que, "*embora as leis e políticas nacionais possam diferir, os países membros têm interesse comum em proteger a privacidade e as liberdades individuais e em conciliar valores fundamentais, mas concorrentes, como privacidade e livre fluxo de informações*"[10].

A resposta parece clara quanto ao **equilíbrio entre valores igualmente relevantes** (fluxo comercial internacional e proteção dos interesses, e também direitos, relacionais a dados pessoais). O obstáculo, no entanto, reside justamente

[10] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. OECD Council Recommendation.

em **atingi-los em alinhamento internacional**. Logo, tendo em vista as potenciais tensões entre ambos objetivos, a viabilidade - e regulação - de tais transferências têm se deslocado - de originalmente uma normatividade específica sobre dados pessoais - para acordos comerciais, seja por meio de instrumentos originalmente nacionais, a exemplo de estruturas contratuais, padrões da ISO[11] ou ainda, mais recentemente, através da criação de *sandboxes* regulatórios;[12] seja por tratados internacionais precipuamente de livre comércio.

Há, portanto, uma busca por preservar os valores e interesses nacionais e igualmente permitir, em paralelo, a existência de fluxo responsável de dados entre jurisdições. Para tanto, os esforços se convergem não apenas na construção de uma necessária **harmonização regulatória** entre Nações plúrimas, mas também se atentar que, no bojo de tais engrenagens, deve-se permitir uma **interoperabilidade de ordenamentos jurídicos.**

Isso porque há uma franca ascensão de fenômenos atrelados à sofisticação de instrumentos técnicos que aumentam a proximidade e multiplicam a intensidade no volume das relações globais, como tecnologias baseadas em *blockchain*, contratos inteligentes, Internet das Coisas (IoT), isso sem falar em emergentes como metaverso. Logo, fronteiras, muros e outros elementos de contenção analogicos simplesmente perdem sua razão de ser, especialmente no que se refere à propagação de informações em sentido amplo.

Cria-se, entretanto, um paradoxo no panorama internacional para as transferências internacionais de dados. Diante de tal infraestrutura tecnológica forjada para existir independente de fronteiras geográficas, baseada na construção de uma estrutura econômica que leva a transações globais, ainda é notória a existência de uma **perspectiva eminentemente**

[11] Sigla em inglês para International Organization for Standardization.
[12] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. Mapping approaches to data and data flows. Report for the G20 Digital Economy Task Force, Saudi Arabia, 2020.

nacional e local aos países, em termos de regulamentação de transferências internacionais.

A título ilustrativo, o art. 3º(3) do Regulamento Geral de Proteção de Dados da União Europeia (GDPR), as regras relativas ao tratamento de dados são aplicáveis a todo e qualquer lugar que se aplique o direito de um país do bloco europeu, "*por força do direito internacional público*", em vistas ao controle de serviços prestados a distância.[13]

Cabe pontuar, nesse sentido, o episódio em 2013 envolvendo as denúncias de Edward Snowden, ex-agente da Agência Nacional de Segurança dos EUA (NSA)[14]. Ao trazer à tona uma série de relatórios confidenciais expondo como o governo estadunidense utilizou as atribuições ligadas à segurança nacional para adotar medidas que permitiram acesso à dados de pessoas ao redor do mundo[15], incluindo invasões à esfera privada de líderes e chefes de Nações soberanas.[16] Nota.se um novo esforço posterior tanto no Brasil como no mundo de regulação e proteção de fluxos internacionais.

Diante da desconfiança instaurada, muitos países demonstraram preocupação na forma de garantir a integridade da segurança cibernética, especialmente, quanto à confidencialidade dos dados pessoais[17]. Surgem, nesse

[13] Interessante notar que no Brasil a regra não aparece nesse mesmo sentido de maneira explícita. De acordo com o art. 3º da Lei Geral de Proteção de Dados (LGPD), o alcance da Lei é aplicável a qualquer localidade em que estejam os dados, física ou virtual, nacional ou estrangeira, desde que: i) a operação de tratamento seja realizado em território nacional; ii) envolva a oferta de bens ou serviços no Brasil; iii) tenha-se tratamento de pessoas localizadas no Brasil ou ainda; iv) os dados tenham sido coletados no Brasil.

[14] Acrônimo em inglês para *National Security Agency*.

[15] Em suas palavras, Snowden aduz que: "*[u]m sistema de vigilância quase universal havia sido estabelecido não apenas sem nosso consentimento, mas também de uma maneira que ocultava deliberadamente de nosso conhecimento todos os aspectos de seus programas*". SNOWDEN, Edward. Eterna vigilância. São Paulo: Planeta, 2019, p. 11.

[16] A teor de reportagem datada de 2014: "*Documentos vazados no ano passado pelo ex-prestador de serviços da Agência de Segurança Nacional (NSA, na sigla em inglês) dos Estados Unidos Edward Snowden indicaram que Dilma e Merkel teriam sido alvo de monitoramento por parte do governo dos EUA*". MATOSO, Felipe. Dilma e Merkel discutirão segurança eletrônica em reunião em Brasília. Disponível em: <https://g1.globo.com/politica/noticia/2014/06/dilma-e-merkel-discutirao-seguranca-eletronica-em-reuniao-em-brasilia.html>. Acesso em: 23.05.2022.

[17] Destaca-se, à época, a proposta conjunta dos governos brasileiro e alemão apresentada à Organização das Nações *Unidas (ONU) visando a criação global de regras para o direito à*

contexto, novas formas de regulação visando maior proteção nacional sobre os dados pessoais. Não por acaso, no Brasil, o Marco Civil da Internet (Lei nº 12.965/14) trouxe previsões relevantes a esse respeito[18]. Como observa Carlos Affonso e Ronaldo Lemos[19]:

> Além do ingresso dos dispositivos sobre privacidade, um segundo tema que passa a constar dos debates sobre o Marco Civil é a possibilidade de se obrigar empresas estrangeiras que coletem dados pessoais de brasileiros a manter servidores no Brasil. Esse dispositivo de localização forçada de dados foi bastante comentado por ser, na época, um desejo expresso do governo federal como resposta aos escândalos de espionagem.

Ocorre que, quanto mais as legislações se desenvolvem no sentido de recrudescer regras e parâmetros ao controle sobre o fluxo transfronteiriço de dados pessoais, maiores são as chances de se caminhar em um sentido diametralmente oposto ao verificado, isto é, de impedir as trocas de bens e serviços.[20] Diante de tais vicissitudes delineadas, nota-se que o panorama global para transferências internacionais de dados parece direcionar à identificação de duas correntes majoritárias.

De um lado, em uma acepção notadamente capitaneada pelos **Estados Unidos**, tem-se que o fluxo de dados pessoais se insere em contexto elementar onde se opera a **primazia da livre circulação de bens e serviços**. Sob esta ótica, a proteção de dados pessoais e o direito à privacidade são

---

privacidade na era digital. G1. Brasil e Alemanha propõem à ONU regras de privacidade na internet. Disponível em: <https://g1.globo.com/politica/noticia/2013/11/brasil-e-alemanha-propoem-onu-regras-de-privacidade-na-internet.html>. Acesso em: 12.01.2023.

[18] A exemplo do art. 11 e seus parágrafos que delimita a observância das legislações brasileiras relativas ao sigilo, confidencialidade e proteção de dados pessoais em operações de tratamento ocorridas em território nacional.

[19] SOUZA, Carlos Affonso; LEMOS, Ronaldo. Marco Civil da Internet: construção e aplicação. Juiz de Fora: Editar, 2016, p. 27.

[20] À época das discussões travadas no plenário do Congresso Nacional ao ainda Projeto de Lei do Marco Civil da Internet, muito se questionou acerca da inclusão de um dispositivo que exigia que empresas estrangeiras que coletassem dados pessoais de brasileiros, mantivessem instalações físicas em território nacional. As motivações inseridas no apogeu dos temores envolvendo os escândalos de espionagem internacional, no entanto, foram em pouco tempo arrefecidas e tiradas de pautas pelo governo, após reconhecer que a previsão poderia resultar em um isolacionismo do país, ao direcionar para uma "localização forçada" de dados.

aspectos relevantes de serem assegurados, desde que compatíveis com a necessária fluidez à realização do comércio internacional.

Dessa maneira, constrições desse panorama se revelam nessa visão como potencialmente prejudiciais ao mundo globalizado e hiperconectado. Isso porque, é inerente às relações internacionais construir um diálogo amplo e aberto, atento às mais diversas realidades e variações socioeconômicas dos países do globo. Nesse sentido, exigir critérios rígidos com o intuito de forjar "estruturas forçadas" à criação de um cenário, simulando a extensão da soberania dos países para que os dados sejam exportados, não é condizente com o necessário alinhamento estratégico à cooperação entre países.

Em paralelo a esta visão, sob uma compreensão especialmente verificada na **União Europeia**, insere-se a interpretação de que, a evolução dada ao direito à privacidade traduz-se na autodeterminação informativa[21]. Logo, há uma busca por efetivo controle sobre o fluxo das próprias informações; o **respeito às liberdades civis e garantias dos direitos dos titulares de dados** são valores que devem ser tutelados em conjunto ao livre desenvolvimento do mercado.

Dessa forma, em razão da proteção de dados ser entendida como um direito humano fundamental, a elaboração de instrumentos e mecanismos para sua tutela é vista como uma condição indispensável à própria viabilidade do comércio internacional. Essas medidas são reverberadas como meios de *compliance* e adequação à sistemática atual dos dados pessoais, de modo que deve-se observar os direitos existentes dos cidadãos daquele país onde seu dado pessoal tenha sido exportado. Afinal, antes de ser um "ativo", o

[21] Conforme o próprio reconhecimento asseverado pelo Tribunal Constitucional Federal alemão (*Bundesverfassungsgericht*), em 1983, que ao invalidar a Lei do Censo de 1982, caracterizado pelo seu potencial dano em criar perfis completos dos cidadãos, reconheceu aos alemães o direito ao controle sobre os próprios dados pessoais, como um pressuposto intrínseco ao direito da personalidade e à extensão conferida à privacidade, em sua tutela positiva.

dado pessoal é um atributo inerente à personalidade humana, sendo merecedor de mesma tutela conferida ao seu titular em território de origem.

Diante de essas abordagens em tensão - potencialmente antagônicas - angariadas por Nações que exercem notória influência na ordem econômica mundial, passa-se ao exame de como os países chegam a acordos no âmbito das transferências internacionais de dados. Para tanto, parte-se inicialmente da identificação se as regras previstas em acordos e tratados internacionais levam à construção de uma estrutura que restringe os fluxos internacionais dados, isto é, podem de alguma maneira obrigar que os dados tenham que estar forçosamente em uma localização geográfica.

3. Transferências internacionais de dados e eventuais limitações aos fluxos transfronteiriços

De um ponto de vista internacional, no cibernético **visualiza-se uma sensível perspectiva de aumento das ações e controle estatal sobre a distribuição de ativos digitais**. Diversos são os fatores que têm levado ao fortalecimento de tal ingerência, tais como pressões por dependências tecnológicas nas mãos de poucos atores no mercado e a escalada de crimes cibernéticos[22]. De todo modo, projetam-se inevitáveis tensões e polarizações, enfraquecendo o alcance de uma circulação mais livre de informações em sentido amplo. O fenômeno passa a ser

[22] MOEREL, Lokke; TIMMERS, Paul. Reflections on Digital Sovereignty. In: EU Cyber Direct, Research in Focus series 2021.

identificado como uma noção de *Soberania Digital*[23] ou ainda de uma *Autonomia Estratégica Digital*[24].

Consequentemente, ainda que as ações não se traduzam em um impedimento às transações comerciais digitais em si, **as dificuldades para a efetivação de um fluxo transfronteiriço de dados pessoais livre podem ser capazes de gerar consequências similares a uma espécie de "*localização forçada*" de dados - "*mandatory data localization*"**. No entanto, o termo pressupõe diferentes intensidades na criação de elementos capazes de gerar limitações às transferências internacionais de dados. Significa dizer que existem "intervenções mais brandas" ou regulações que criam constrições o que de certa forma suaviza obrigações de localização (um "*localização suave*"), ainda que na prática essas restrições existam de igual maneira[25].

Dados sugerem que somente no ano de 2021, 92 medidas em 39 países ao redor do mundo exigiam explicitamente que os dados fossem armazenados ou processados internamente[26]. Nota-se ainda que mais da metade dessas medidas surgiram nos últimos cinco anos, o que sugere tratar-se de um fenômeno em pleno recrudescimento, dificultando as perspectivas de cooperação no atual contexto de

[23] Conforme conceitua a reportagem veiculada recentemente pelo jornal The New York Times: "Impulsionados por preocupações com segurança e privacidade, bem como interesses econômicos e impulsos autoritários e nacionalistas, os governos estão cada vez mais estabelecendo regras e padrões sobre como os dados podem e não podem se movimentar pelo mundo. O objetivo é ganhar 'soberania digital'". Tradução livre. MCCABE, David; SATARIANO, Adam. The Era of Borderless Data Is Ending. Disponível em: <https://www-nytimes-com.cdn.ampproject.org/c/s/www.nytimes.com/2022/05/23/technology/data-privacy-laws.amp.html>. Acesso em: 25.05.2022.

[24] Para Lokke Moerel e Paul Timmers o conceito Autonomia Estratégica Digital soa mais condizente a um "um conceito que se originou no pensamento militar/de defesa, mas agora é visto como 'as capacidades e capacidades de decidir e agir de forma autônoma em aspectos essenciais do futuro de longo prazo na economia, sociedade e democracia'". Tradução livre. MOEREL, Lokke; TIMMERS, Paul. Op cit.

[25] ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN. Internet & Jurisdiction and ECLAC Regional Status Report 2020. Santiago: United Nations Publications, 2020, p. 114.

[26] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. A Preliminary Mapping of Data Localisation Measures. OECD Trade Policy Papers, N. 262, OECD Publishing, Paris, 2022.

enfrentamento dos efeitos causados pela pandemia de covid-19.

3.1. Restrições nacionais

Em países como **China, Rússia e Irã**, intervenções estatais sobre suas economias e sociedades verificadas a partir de políticas públicas mais expressivas, resultam em mecanismos congêneres no tocante à economia digital[27]. Os governos desses países atuam ativamente no **controle exercido sobre o fluxo de informações que circulam suas jurisdições, construindo um cenário de limitações aos pressupostos de uma livre saída dos dados**[28].

Enquanto a China avança na competitividade de liderança como desenvolvedora de soluções tecnológicas, legislações internas sobre privacidade e cibersegurança impõem instrumentos pautados no armazenamento de instalações físicas no país. Nessa lógica, para que se operem transações comerciais é necessário ainda o escrutínio do Governo Central de todas as informações angariadas[29].

Embora não seja um líder tecnológico como o país vizinho, o modelo russo de circulação de dados é bastante similar ao chinês, pautado na centralidade da segurança da rede e dos dados como uma questão política e de segurança nacional. Para que empresas operem no país, exige-se que as companhias "*registrem, sistematizem, acumulem, armazenem, alterem, atualizem e recuperem dados pessoais de todos os*

[27] Como se destaca, a título de exemplo, de relatório conduzido por pesquisadores da Information Technology and Innovation Foundation (ITIF): "Digital authoritarian governments—led by China and Russia—see physical access to data centers as a critical enabler of surveillance and political control. Data localization enables political oppression by bringing information under government control and allowing the government to identify and threaten individuals, thereby impacting privacy, data protection, and freedom of expression". CORY, Nigel; DASCOLI, Luke. How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Disponível em: <https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/>. Acesso em: 12.01.2023.

[28] SHERMAN, Justin; TRIPLETT, Holden. Why Russia, China, and Other Countries Are Demanding Big Tech Companies Build Local Offices. Disponível em: <https://slate.com/technology/2022/02/data-localization-laws-china-russia-authoritarian.html>. Acesso em: 05.06.2022.

[29] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. Op cit.

cidadãos russos, usando servidores russos", conforme determina a lei federal local[30].

Perto dali, do outro lado do Mar Cáspio, o Irã, também vem adotando medidas arbitrárias também capazes de pôr em xeque um fluxo livre de dados. Já existem diversas plataformas populares banidas, como Facebook, Twitter, YouTube, TikTok e Telegram, além de milhões de sites bloqueados[31]. Atualmente, tramita um projeto de lei voltado a criminalizar o uso de VPNs (*Virtual Private Networks*)[32], ferramenta dotada de proteção criptográfica essencial à atuação e proteção de ativistas, jornalistas e agentes humanitários em países com viés antidemocrático.

Recentemente, mudanças legislativas na **Índia** têm gerado preocupações especialmente por estratégicos aliados como os EUA, por estipularem **regras que podem levar a que empresas estrangeiras se sintam obrigadas a se instalarem em território indiano** para que as operações envolvendo o processamento de dados pessoais sejam viabilizadas[33]. Diversas associações civis e empresas de tecnologia têm se posicionado, alertando sobre os possíveis impactos socioeconômicos aptos a se deflagrar, em meio a custos capazes de encerrar operações e isolar, ao menos digitalmente, os quase 1,4 bilhão de cidadãos indianos. No entanto, as motivações por detrás de tal movimentação indiana é na narrativa contra possíveis restrições à "soberania do país", isto é, **impedir com que os países desenvolvidos obtenham benefícios dos fluxos de dados transfronteiriços em detrimento aos interesses nacionais**[34].

---

[30] Ibid.

[31] ZIABARI, Kourosh. Iran's Leaders Are Scared of the Internet. Disponível em: <https://foreignpolicy.com/2022/06/06/iran-internet-protection-bill-curbs-restrictions-unrest/>. Acesso em: 16.01.2023.

[32] Ibid.

[33] THE CENTRE FOR INTERNET AND SOCIETY, INDIA. The Localisation Gambit Unpacking Policy Measures for Sovereign Control of Data in India, 2019.

[34] UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT. Digital Economy Report 2021: Cross-border data flows and development: For whom the data flow. Nova York: United Nations Publications, 2021.

3.2. Restrições indiretas

De certa forma, em parte, pode-se observar em alguns países e regiões o levantamento de critérios e procedimentos que podem ser a uma situação com efeitos similares. Na União Europeia, por exemplo, para que se opere a exportação de dados do Espaço Econômico Europeu (EEE)[35] há a necessidade de alinhamento frente a uma série de critérios e mecanismos. Em um primeiro nível, tem-se a exportação para países contemplados com decisões de adequação, considerados como possuindo um nível "equivalente de proteção de dados" ao existente no contexto europeu, nos termos do art. 45, do GDPR[36].

Subsidiariamente, na forma do art. 46, GDPR, existem regras relativas à apresentação de garantias adequadas, a exemplo de regras vinculativas aplicáveis às empresas, cláusulas-padrão contratuais ou ainda outros instrumentos juridicamente vinculativos[37]. Mas, por estarem sujeitas embasados em uma efetiva proteção, estes regramentos se encontram sob frequentes reconsiderações. Não à toa, nos termos do art. 46(5), GDPR, autorizações concedidas pelas Autoridades Nacionais de Proteção de Dados (DPAs) sob a égide da primeira legislação sobre o tratamento de dados da União Europeia, a Diretiva 95/46/CE, "*continuam válidas até que a mesma autoridade de controlo as altere, substitua ou revogue, caso seja necessário*".

---

[35] "*O RGPD aplica-se no Espaço Económico Europeu (EEE), que inclui todos os países da UE e ainda a Islândia, o Listenstaine e a Noruega. Quando os dados pessoais são transferidos para fora do território do EEE, as proteções concedidas pelo RGPD viajam com esses dados. Isto significa que, para exportarem dados para o estrangeiro, as empresas têm de assegurar a aplicação de determinadas garantias*". COMISSÃO EUROPEIA. O RGPD: novas oportunidades, novas obrigações. Luxemburgo: Serviço das Publicações da União Europeia, 2018, p. 15.

[36] Nos termos do art. 45, GDPR, compete à Comissão Europeia a prerrogativa de determinar, alterar, revisar ou revogar decisões que avaliem se um país fora da União Europeia oferece um nível adequado de proteção de dados pessoais. EUROPEAN COMMISSION. Adequacy decisions. Disponível em: <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en >. Acesso em: 16.01.2023.

[37] Importante destacar a inspiração da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18) à estrutura do GDPR, especialmente neste sentido de gradações para que as transferências internacionais sejam autorizadas.

Talvez um dos exemplos mais notórios desta perspectiva de proteção equivalente concreta se encontra na tensão sobre os mecanismos de transferência internacional de dados estabelecidos entre a União Europeia e os Estados Unidos. Originalmente considerado um "país adequado" por uma decisão de adequação da União Europeia datada de 2000, ainda no bojo da Diretiva 95/46/CE, o fluxo transfronteiriço de dados pessoais entre as Nações do Oceano Atlântico Norte era tinha como base um mecanismo estabelecido no acordo intitulado "*Safe Harbor*". A decisão de adequação, no entanto, foi invalidada pela Corte de Justiça da União Europeia (CJUE) em 2015, consoante precedente histórico popularmente conhecido como *Schrems I*[38], em razão de o mecanismo previsto no acordo e que dava azo à decisão não ser suficiente para proteger os direitos de cidadãos europeus[39].

Em uma nova investida, em 2016, as Partes fizeram esforços em uma nova tratativa, então denominada *Privacy Shield*, trazendo regras mais claras quanto ao respeito à privacidade dos titulares de dados[40]. Mas em 2020, a CJUE asseverou novamente a invalidade da nova decisão da Comissão, agora baseada nesse segundo acordo. O caso, denominado *Schrems II*, baseou-se em circunstâncias semelhantes ao precedente anterior, em que as ingerências promovidas pelos EUA ainda demonstravam graves preocupações à segurança

[38] No caso em comento, o ativista austriaco Maximillian Schrems moveu uma ação judicial questionando o cumprimento de empresas estadunidenses quanto à proteção de dados oriundos da UE e transferidos para os EUA no bojo do Safe Harbor Agreement, diante de preocupações de espionagem por parte de agências de inteligência dos EUA. O acordo, baseado em uma série de princípios de proteção de dados, previa que empresas americanas poderiam se inscrever de forma voluntária para operar as transferências internacionais de dados, de modo que a proteção conferida aos titulares dependia de autoavaliação e autocertificação das próprias entidades, não demonstradas no caso concreto.

[39] Destaca-se ainda que de acordo com as regras de territorialidade do GDPR, para além da proteção de cidadãos europeus situados fora da União Europeia, a normativa também protege qualquer titular residente em território da União.

[40] Nos termos do novo acordo, para além da principiologia elementar à proteção de dados pessoais, exigia-se um forte conjunto de requisitos e salvaguardas necessárias à prévia transferência internacional dos dados da UE para os EUA.

das informações pessoais[41], pois os dados oriundos da UE que houvessem sido exportados para os EUA, mesmo que dentro do *Privacy Shield*, não possuiriam nível "equivalente" de proteção.

Mais recentemente, em 2022, os Estados Unidos e a União Europeia deram um passo à frente rumo à formalização de um novo acordo, ao menos em teoria, agora intitulado *Trans-Atlantic Data Privacy Framework*. Dentre os novos objetivos destacam-se: (i) regras mais rígidas às empresas ao transferirem dados pessoais da UE para os EUA; (ii) limitações mais claras quanto ao escrutínio de agências de inteligências americanas sobre os dados pessoais e ainda; (iii) a criação de uma Corte de de Revisão de Proteção de Dados para solucionar demandas de cidadãos europeus quanto ao uso de dados em território americano.

Como consequência direta, as relações comerciais no Atlântico Norte foram arrefecidas, provocando restrições e até mesmo proibições na prestação de serviços estadunidenses, que dependiam das transferências para manter suas operações em funcionamento. A exemplo, nesse sentido, de decisões proferidas por Autoridades nacionais de Proteção de Dados europeias, como as da Áustria, França e Portugal.

3.3. Acordos que visam regular obrigações de localização forçada

Constituído como um dos acordos mais antigos em termos de proteção de dados pessoais, logo após o estabelecimento das Diretrizes da OCDE vista em alhures, a Convenção 108 do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, é datado de 1981. Nos termos do art. 12, uma Parte

[41] EUROPEAN COMMISSION. European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087>. Acesso em: 30.05.2022.

não pode proibir ou sujeitar à autorização especial fluxos transfronteiriços de dados pessoais com destino ao território de outra Parte. Nada obstante, autoriza-se aos países adotarem medidas necessárias à segurança no tratamento automatizado de dados e ainda no que toca a categorias especiais de dados.

Ainda mais recentemente, a Convenção 108+ atualizou-se em 2018, contemplando novos países membros e modernizando seus dispositivos. A exemplo do Capítulo III sobre fluxo transfronteiriço de dados pessoais, que autoriza a transferência internacional de dados em hipóteses como: (i) quando prevalecerem interesses legítimos; (ii) interesses públicos importantes (art. 14, 4, c) e ainda; (iii) se constituir uma medida necessária e proporcional em uma sociedade democrática para a liberdade de expressão (art. 14, 4, d).

Em meio à crescente perspectiva de cercear direta ou indiretamente as formas de continuidade dos fluxos transfronteiriços de dados pessoais, cabe pontuar que existem acordos voltados à coibição destas práticas.

No contexto sul-americano, o Acordo Sobre o Comércio Eletrônico do Mercosul. Nos termos da Decisão nº 15/20, Argentina, Brasil, Paraguai e Uruguai se comprometem a enveredar os melhores esforços para que se tenha a livre circulação de bens no comércio digital, incluindo desembaraços de natureza alfandegária (art. 3º), bem como quanto à validade de assinaturas eletrônicas (art. 4º). Ainda, é reconhecida a legitimidade das Partes signatárias terem seus próprios requisitos regulatórios para segurança para transferências de informações eletrônicas, incluindo o uso de instalações informáticas. No entanto, tal possibilidade não pode ser capaz de criar medidas incompatíveis aptas a causar discriminação arbitrária, injustificável ou uma restrição encoberta ao comércio, inclusive com relação à proteção de dados pessoais, tal como exigir que uma das Partes tenha que **usar ou estabelecer instalações informáticas no território de outra para que realizem as atividades eletrônicas** (arts. 7º).

Em sentido similar, o Acordo Bilateral de Livre Comércio entre Brasil e Chile (DL nº 288/21), estipula uma série de regulamentações quanto ao comércio amplo de bens e serviços entre os dois países sul-americanos. Quanto às definições para o comércio eletrônico (art. 10), autoriza-se que as Partes estabeleçam suas regulações, justificáveis e não arbitrárias, para a garantia e confiabilidade das comunicações. Além disso, uma Parte não pode exigir que a outra precise **usar ou estabelecer instalações informáticas em seu território como condição para a realização de negócios**.

Por sua vez, os países signatários da Cooperação Econômica Ásia-Pacífico (APEC)[42], que tem como objetivo estabelecer o livre comércio nas Nações que margeiam o Oceano Pacifico, possuem regras muito expressivas quanto às transferências internacionais de dados[43]. Estimulam-se as práticas para que o fluxo transfronteiriço de dados seja permitido entre as Nações, em vistas à responsabilidade de cada agente, no caso concreto, atuar em prol do atendimento às leis locais de privacidade e proteção de dados (item III, 66). Ainda, estabelece-se que as Partes signatárias devem se **abster de restringir os fluxos transfronteiriços de dados**, especialmente considerando a existência de leis de proteção de dados locais ou existam salvaguardas suficientes adotadas pelos Controladores, garantindo um nível de proteção adequado. Além disso, quaisquer restrições eventualmente adotadas devem ser proporcionais aos riscos identificados, levando em consideração a finalidade e a sensibilidade das informações pessoais (item IV, 69 e 70).

Na América do Norte, ao renovar o então acordo de livre comércio intitulado NAFTA[44], o novo Acordo Estados Unidos-México-Canadá (USMCA)[45] trouxe novas regulações

[42] Acrônimo em inglês para Asia-Pacific Economic Cooperation.

[43] A exemplo do denominado Marco da Privacidade, que contém orientações, diretrizes e fundamentos relevantes à perspectiva da harmonização normativa entre os países. APEC. Privacy Framework. Disponível em: <https://cbprs.blob.core.windows.net/files/2015%20APEC%20Privacy%20Framework.pdf>. Acesso em: 16.01.2023.

[44] Acrônimo em inglês para North American Free Trade Agreement.

[45] Acrônimo em inglês para United States-Mexico-Canada Agreement.

de setores comerciais, dentre eles, um capítulo próprio ao Comércio Eletrônico. Ao reconhecerem a validade das regras relativas às transferências internacionais de dados dadas pela APEC, os países norte-americanos asseveram que nenhuma Parte pode proibir ou restringir o fluxo transfronteiriço de dados, incluindo em sua perspectiva eletrônica, para a condução de negócios. No entanto, conforme art. 19.11, autoriza-se a adoção de medidas legítimas à manutenção da ordem pública, desde que não seja criado um mecanismo arbitrário ou injustificável à restrição de comércio ou ainda que não imponha medidas restritivas às transferências internacionais de dados superiores ao objetivo necessário.

Após a saída do Reino Unido da União Europeia (UE), nota-se que o Acordo de Comércio e Cooperação adotado entre as Nações europeias trouxe uma estrutura bem rígida e definida quanto às vicissitudes do intenso comércio local[46]. Consoante art. 201º, pressupõe-se que o fluxo transnacional de dados não seja restringido por nenhuma das Partes, sobretudo quanto às exigências de: (i) utilização de equipamentos informáticos no território nacional; (ii) localização de dados no território nacional para armazenamento; (iii) proibição ao armazenamento ou tratamento de dados no território nacional ou que ainda; (iv) condição à utilização de aparelhos informáticos em território nacional.

No tocante às relações comerciais da UE com outras Nações, destaca-se também o Acordo de Parceria Econômica celebrado com o Japão. Nos termos do capítulo de serviços financeiros, o art. 8.63 define que uma Parte não poderá adotar medidas que impeçam as transferências de informações ou processamento de informações financeiras por meios eletrônicos. Do mesmo modo, não é permitido que, sob eventuais regras de importação, impeçam-se transferências de equipamentos, caso tais transferências envolvam informações necessárias à condução de negócios formais. No entanto, autoriza-se que as Partes adotem as

[46] Cumpre ressaltar que a existência de um prazo de 3 anos para que as Partes acompanhem o funcionamento do acordo, facultando-se o direito de cada uma das Partes revisarem a lista de restrições ao fluxo transfronteiriço de dados (art. 201º(2).

medidas necessárias para a garantia da confidencialidade dos dados pessoais, especialmente relativos a registros e contas individuais.

3.4. Acordos que apenas abordam a importância da proteção de dados pessoais e a livre circulação

Na América Central, observa-se que no âmbito do Mercado Comum e Comunidade do Caribe (CARICOM)[47], as nações que margeiam o Mar do Caribe buscam desenvolver diversos setores econômicos. Para tanto, são previstos requisitos para transferências internacionais de recursos tecnológicos para a política industrial local (art. 51), bem como informações tecnológicas para a promoção de assistência técnica e financeira (art. 157). No entanto, define-se que todos os dispositivos que orientam o compartilhamento de bens e serviços não devem ser interpretados no sentido de obrigar os Estados-Membros a fornecer informações contrárias aos seus interesses de segurança (art. 225).

Em outro Acordo de Livre Comércio, pactuado entre a UE e a Coréia do Sul, as partes reconhecem a adoção de mecanismos necessários para o fluxo transfronteiriço de informações. Mas especialmente no Anexo 7-D, destaca-se que a Coréia do Sul se compromete a alterar suas regulamentações internas, em vistas à **maior permissão de transferências de informações financeiras**, tutelando igualmente a proteção dos dados pessoais necessários.

Especificamente no continente asiático, por meio da Associação das Nações do Sudeste Asiático (ASEAN)[48], acordo voltado ao desenvolvimento econômico e político local, as Nações possuem um Acordo de Telecomunicações e Informações de Tecnologia. O regramento, no entanto, é bastante focado à garantia de princípios mínimos relacionados à proteção de dados, e, no que toca às

[47] Sigla em inglês para *Caribbean Community*.
[48] Sigla em inglês para *Association of Southeast Asian Nations*.

transferências internacionais de dados, obriga as organizações a obterem **prévio consentimento dos titulares de dados** para esta finalidade ou que adote medidas necessárias para que empresas protejam os dados pessoais de forma consistente à principiologia adotada (item 6, "f").

No âmbito da União Africana, nota-se que a Convenção sobre Segurança Cibernética e Proteção de Dados Pessoais possui delimitações claras em prol do desenvolvimento da proteção de dados no continente. A partir de disposições como limitação aos serviços eletrônicos (arts. 1 a 7), obrigação a constituição de autoridades nacionais de proteção de dados nos países (arts. 11 e 12) e a regulamentação interna de países quanto aos direitos dos titulares de dados (arts. 13 a 23). Especificamente com relação ao combate ao crime cibernético, fala-se em transferência internacional de dados **unicamente para a necessária cooperação nas atividades investigativas** (art. 28).

Conforme ainda o Acordo de Livre Comércio entre Singapura e Austrália, nota-se que as Partes adotam um capítulo próprio à cooperação da Economia Digital. Sob uma perspectiva inovadora, as Nações se comprometem a adotar um *sandbox* regulatório[49] em prol de transferências internacionais de dados, de maneira a promover a inovação de dados (art. 26), além de desenvolver uma política de dados abertos entre os governos (art. 27). Reconhecem tambem a validade das regras para as transferências internacionais de dados, nos termos definidos pela APEC, mas nenhuma das Partes poderá restringir as transferências de forma arbitrária ou discriminação injustificável à restrição comercial (art. 23). Além disso, é vedada a exigência por uma das Partes de usar ou

[49] Apesar das dificuldades de implementação, "*as oportunidades que os sandboxes transfronteiriços podem criar são significativas. Sandboxes que lidam com dados podem melhorar a segurança regulatória, melhorar os fluxos de dados e permitir que empresas novas e inovadoras tenham melhor acesso a clientes e serviços no exterior. Do ponto de vista do regulador, eles poderiam reduzir a arbitragem regulatória e o fórum-shopping e construir uma conformidade mais consistente, com base no apoio mútuo, colaboração e alinhamento entre os reguladores envolvidos*". Tradução livre. DATASPHERE. Sandboxes for data: creating spaces for agile solutions across borders. Disponível em: <https://www.thedatasphere.org/datasphere-publish/sandboxes-for-data/>. Acesso em: 07.06.2022

manter instalações de computação no território de uma das Partes como condição à realização de negócios (art. 24).

A perspectiva de criação de *sandboxes* regulatórios também se destaca no Acordo de Parceria da Economia Digital (DEPA)[50] celebrado entre Chile, Nova Zelândia e Singapura. Nos termos do art. 9.4, as Partes reconhecem a relevância do fluxo transfronteiriço de dados pessoais permitindo a construção de inovação, apta a ser aperfeiçoada por meio do *sandbox* regulatório que autoriza o compartilhamento de dados, em paralelo ao respeito às legislações de cada país.

Dessa forma, pode-se afirmar que apesar de possíveis restrições observadas em países como China, Rússia e Índia, construídas sob propósitos diferentes, ou ainda, diante de modulações indiretas identificadas na União Europeia, há uma forte visão para ter em tratados e acordos internacionais obrigações nos seguintes sentidos:

[50] Sigla em inglês para The Digital Economy Partnership Agreement.

Nacionalismo Digital	Circulação **condicionada**	Circulação **livre**	Construção ou sofisticação da **cultura de dados**
Interesses nacionalistas preponderantes, associados ou não a uma política de "Soberania Digital", seja por motivações vistas como autoritárias, seja por preocupações quanto à possível subordinação aos países de industrialização antiga..	As preocupações ligadas à proteção de dados pessoais tendem a prevalecer sobre a manutenção de acordos internacionais, especialmente, sob uma visão de continuidade do acordo, enquanto perdurarem as condições que deram azo ao acordo originalmente.	Os países mantêm esforços de modo a proibir expressamente mecanismos que levam a consequências associadas a uma "localização forçada", em prol da harmonia e confiança depositadas.	As perspectivas ligadas à simetria de interesses, seja por ainda ser necessário o desenvolvimento de uma cultura protetiva de dados, seja por já estarem sob um forte e recíproco panorama de proteção de dados, levam a apenas autorizar ou aperfeiçoar o fluxo de dados pessoais.

Em certa medida, as diferentes gradações relacionadas ao controle no fluxo de dados estão diretamente relacionadas à existência de tratativas multilaterais amadurecidas que permitem o fluxo de dados entre as Nações. A exemplo dos países membros da OCDE, notadamente formados por países do Norte Global, cerca de 60% das medidas relacionadas a regulação ou controle de dados envolvem apenas requisitos de armazenamento local nos territórios para viabilizar o fluxo[51]. Noutro giro, em países não-membros da OCDE, 83% das medidas estão associadas a requisitos de armazenamento com proibições de fluxo de dados[52].

[51] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. A Preliminary Mapping of Data Localisation Measures. OECD Trade Policy Papers, N. 262, OECD Publishing, Paris, 2022.
[52] Ibid.

4. Colocando o “pingo nos is”: qual o propósito dos principais tratados e acordos

Apresentados os principais tratados e acordos internacionais e suas respectivas regulações e eventuais limitações ao fluxo transfronteiriço de dados, passa-se ao exame sobre o que os documentos internacionais visam efetivamente abordar. Para tanto, parte-se de 5 pontos analíticos a partir de elementos que possam a dar contornos aos seus respectivos alcances.

4.1. Como regra, as transferências são autorizadas?

Diante de notáveis impasses quanto à construção de mecanismos que cerceiam a livre circulação de dados direta ou indiretamente, passa a ser necessário identificar se efetivamente as transferências internacionais de dados são autorizadas no bojo dos tratados e acordos internacionais identificados.

Como observado na seção anterior, nota-se que o fluxo transfronteiriço de dados em tais documentos internacionais em regra são não apenas autorizadas, como também muitas vezes estimuladas para que se atinja as finalidades previstas nos objetivos variados entre as Nações. Importa destacar que tais instrumentos jurídicos partem de um amplo alinhamento, em que as transferências internacionais de dados se inserem como elementos essenciais a esses interesses sociais e/ou econômicos recíprocos entre os países.

4.2. Faz-se relação com algum padrão ou normativa específica?

Diante do constatado anteriormente, nota-se que alguns tratados internacionais fazem alusão a regras e determinados padrões para que sejam autorizados o intercâmbio de dados.

No âmbito do Capítulo Comércio Eletrônico da USMCA, por exemplo, o art. 19.5 obriga as Partes a adotarem uma estrutura normativa para a governança de transações eletrônicas de forma consistente aos princípios da Lei Modelo de 1996 da UNCITRAL sobre o Comércio Eletrônico. Ainda, consoante art. 19.8, as Partes reconhecem que o sistema de Regras de Privacidade Transfronteiriça da APEC como um mecanismo válido para facilitar as transferências de informações transfronteiriças enquanto protege as informações pessoais.

Em sentido similar, o Capítulo Economia Digital do Acordo de Livre Comércio entre Singapura e Austrália, faz referência às mesmas regras da APEC e às Diretrizes que regem a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais da OCDE, na qualidade de instrumentos adequados à proteção e transferência de dados pessoais (art. 17).

Na maioria, no entanto, não há uma referência a um padrão internacional específico a ser seguido relegando outros fatores.

4.3. Cria-se uma norma ou outorga-se a regulação nacional interna?

Em alguns casos o padrão estabelecido no âmbito dos tratados e acordos internacionais para a regulação da proteção de dados determina o estabelecimento de uma norma ou remete a uma regulação doméstica. Nota-se que existem algumas variações, a depender especialmente do nível de amadurecimento do país em termos de proteção de dados pessoais, além da existência de muitos países

signatários de acordos com estruturas jurídicas muito variáveis entre si.

Nos termos da Convenção sobre Segurança Cibernética e Proteção de Dados Pessoais celebrada pela União Africana, nota-se a perspectiva de construção de uma cultura de proteção de dados pessoais. Isso porque, delimita-se de forma mais expressiva a necessidade dos países membros de desenvolverem seus próprios marcos legais de proteção de dados, levando em consideração os princípios e direitos elencados na convenção como relevantes, bem como a constituição de autoridades nacionais de proteção de dados, para a plena cooperação entre as Partes signatárias.

Ainda, nos termos do Marco de Privacidade da APEC, as Partes signatárias delimitam uma seção própria com um Guia para Implementação Doméstica, incluindo aperfeiçoamento das legislações de proteção de dados, para a consequente fluidez necessária ao fluxo transfronteiriço (parte IV, seção A).

4.4. Trata da regulação de serviços em nuvem?

A perspectiva de computação em nuvem está diretamente relacionada ao fluxo transfronteiriço de dados pessoais. Para que os dados sejam armazenados em âmbito íntegro e seguro, mantido por servidores terceirizados, muitos países dependem da exportação de dados para que sejam tratados internacionalmente[53].

Nem todos os países têm a capacidade instalada internamente com servidores com flexibilidade de escala para a realização dos tratamentos que necessitam. Esse é o caso do Brasil em que existe capacidade nacional, mas

[53] Nesse sentido: "*Apesar de a nuvem ser descrita como algo abstrato, distante e obscuro, na realidade ela utiliza o computador físico, com instalações de armazenamento físico alojadas em estruturas físicas que podem estar sujeitas a uso indevido. Isso requer procedimentos adequados de proteção de dados para garantir a privacidade e a segurança de tais dados*". Trad. livre. TEHRANI, P. M.; SABARUDDIN, J. S. B. H.; RAMANATHAN, D. A. P. Cross border data transfer: Complexity of adequate protection and its exceptions. In: Computer Law & Security Review, n 31, 2018, p. 582-594. https://doi.org/10.1016/j.clsr.2017.12.001

muitas vezes há o uso direto ou subsidiário de empresas cuja nuvem está em território estrangeiro.

Como visto no caso envolvendo os conflitos entre os EUA e UE no tocante às idas e vindas de um acordo que viabilizasse o fluxo transfronteiriço de dados, a ausência de um alinhamento mútuo trouxe impactos significativos, inclusive em certas circunstâncias levou à interrupção de diversos serviços de nuvens que eram oferecidos por empresas americanas no contexto europeu[54]. Afinal, embora as nuvens gerem uma noção de diminuição em termos de análise e armazenamento de dados, é mais do que corriqueiro a necessidade de envio das informações a outras jurisdições para que a atividade seja economicamente viável.

Assim, muito embora não haja menções expressas ao termo "*nuvem*" ou ainda à "*computação em nuvem*", alguns tratados e acordos delimitam a vedação quando eventuais exigências de instalações informáticas em territórios nacionais, como condição para realização de negócios envolvendo o compartilhamento de dados pessoais, a exemplo do Acordo Sobre o Comércio Eletrônico do Mercosul (art. 8º), Acordo Bilateral de Livre Comércio entre Brasil e Chile (art. 10.13), Capítulo Comércio Eletrônico da USMCA (art. 19.12) e o Acordo de Comércio e Cooperação (art. 201º). Significa dizer que, em comum, tais dispositivos versão redação similar determinando que "*uma Parte não poderá exigir de uma pessoa de outra Parte que use ou estabeleça as instalações informáticas no território dessa Parte como condição para a realização de negócios nesse território*"[55].

[54] LOMAS, Natasha. Legal clouds gather over US cloud services, after CJEU ruling. Disponível em: <https://techcrunch.com/2020/07/17/clouds-gather-over-us-cloud-services-after-cjeu-ruling/>. Acesso em: 27.06.2022.

[55] A exemplo do dispositivo literal contido no art. 8º do Acordo Sobre o Comércio Eletrônico do Mercosul.

4.5. Há um vínculo com regulações setoriais?

Percebe-se que, de forma geral, os tratados e os acordos vinculam-se à ampla tutela de questões sociais e econômicas. Nesse sentido, alguns tratados possuem capítulo específico à transferência internacional de dados, especialmente no contexto eletrônico, como no caso da USMCA, com seu Capítulo Comércio Eletrônico e ainda o Capítulo Economia Digital no Acordo de Livre Comércio entre Singapura e Austrália.

Há, decerto, expressiva orientação para que os dados pessoais especialmente financeiros sejam regulados em apartado, em atenção à viabilidade do comércio de bens e serviços. Esse panorama é interessante, tendo em vista que, ao se analisar as principais categorias de dados pessoais relacionadas às medidas de controle sobre o fluxo transfronteiriço, dados de transações comerciais, dados financeiros e dados de pagamentos são os principais alvos de restrições, respectivamente, 17%, 12% e 7%[56].

A exemplo de tratativas específicas, nota-se a existência de regulações setoriais mais específicas, a exemplo do Acordo Sobre o Comércio Eletrônico do Mercosul, versando sobre o *e-commerce* no contexto sul-americano, o Acordo de Telecomunicações e Informações de Tecnologia da ASEAN, que se ocupa à tutela de transferências apenas no contexto de transmissões de radiodifusão e telecomunicações. Ainda, sob a Convenção sobre Segurança Cibernética e Proteção de Dados Pessoais da União Africana, nota-se uma clara proposição direcionada ao desenvolvimento da proteção de dados no continente, assim como o estabelecimento de uma cooperação multinacional à cooperação para combate ao cibercrime.

[56] ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT. A Preliminary Mapping of Data Localisation Measures. OECD Trade Policy Papers, N. 262, OECD Publishing, Paris, 2022.

Um seguinte quadro esquemático no tocante aos pressupostos dos tratados e acordos internacionais pode ser identificado:

	As transferências são autorizadas?	Há referência a um padrão ou normativa específica?	Cria-se uma norma ou outorga-se a regulação interna?	Fala-se em nuvem?	Vincula-se a regulações setoriais?
Acordo Sobre o Comércio Eletrônico do Mercosul	✅	❌	❌	❌	✅
Acordo Bilateral de Livre Comércio entre Brasil e Chile	✅	❌	❌	❌	❌
Mercado Comum e Comunidade do Caribe (CARICOM)	✅	❌	❌	❌	❌
Convenção 108 do Conselho da Europa	✅	❌	❌	❌	❌
Cooperação Econômica Ásia-Pacífico (APEC)	✅	✅	✅	❌	❌
Acordo Estados Unidos-México-Canadá (USMCA)	✅	✅	❌	❌	❌
Associação das Nações do Sudeste Asiático (ASEAN)	✅	✅	❌	❌	❌
Convenção sobre Segurança Cibernética e Proteção de Dados Pessoais da União Africana	✅	❌	✅	❌	✅
Acordo de Comércio e Cooperação (UE-R.U.)	✅	❌	❌	❌	❌
Acordo de Parceria Econômica (UE-Japão)	✅	❌	❌	❌	❌

Acordo de Livre Comércio (UE-Coréia do Sul)	✅	❌	❌	❌	❌
Acordo de Livre Comércio (Singapura-Austrália)	✅	✅	❌	❌	❌
Acordo de Parceria da Economia Digital (Chile, Nova Zelândia e Singapura)	✅	❌	❌	❌	❌

5. Considerações finais

Com base nas questões acima delineadas, buscou-se identificar os pressupostos por detrás de tratados e acordos internacionais e a consequente regulação transfronteiriça de dados pessoais. A partir do quadro normativo, é possível concluir que **os diversos acordos celebrados entre as Nações do globo, como regra, autorizam as transferências internacionais de dados**, mesmo diante de oscilações quanto aos parâmetros inerentes à viabilidade do intercâmbio de dados, a partir de regras mais rígidas ou mais flexíveis. Os principais tratados e acordos tendem assim a buscar a interoperabilidade de sistemas jurídicos internacionais.

O Brasil deve se encaixar de alguma forma nesse panorama. Tendo em vista que a Agenda Regulatória 2022-2023 da Autoridade Nacional de Proteção de Dados que dá continuidade à discussão do tema e prevê que as definições para as transferências internacionais de dados deverão ser regulamentadas. Acredita-se que o presente relatório possa influenciar positivamente a perspectiva regulatória nacional. Deve-se ter em mente, no âmbito da iminente regulamentação nacional, perspectivas adequadas ao melhor equilíbrio entre direitos socialmente relevantes, juntamente com o diálogo aberto à perspectiva de confiança e compatibilização com os demais países.

Nota-se uma direta relação da **fluidez da interoperabilidade de dados entre países e o desenvolvimento do comércio internacional**. Para tanto, uma adequada perspectiva se pauta no equilíbrio funcional entre a proteção de dados pessoais e a possibilidade de se encontrar mecanismos para que esses dados possam circular livremente. Identifica-se, portanto, duas principais consequências quanto à existência de muitas barreiras: (i) eventual restrição excessiva quanto à saída de dados gerará uma considerável diminuição na participação do comércio internacional ou ainda; (ii) por sempre existirem critérios potencialmente ilegítimos que impactam à exportação de dados, sendo que o fluxo encontrará outros meios à sua circulação, que não aqueles previstos pelo legislador.

Como salientado por Elizabeth Denham, diretora da Autoridade Nacional de Proteção de Dados do Reino Unido (ICO)[57], o mundo deveria estar reunindo esforços em prol de um "*Bretton Woods* de dados". O termo faz alusão à Conferência de Bretton Woods, realizada em 1944, onde 45 países assinaram diversos acordos comprometendo-se à cooperação internacional, por meio de ajustes monetários visando à expansão comercial e facilitação de negociações cambiais no mundo.

Nesse mesmo contexto, de modo a evitar a dependência de uma gama de acordos e tratativas variadas e complexas entre as diversas Nações, deve-se refletir quanto à necessária facilitação na troca de dados pessoais, especialmente diante da digitalização das relações humanas. Nas palavras da Diretora da ICO: "*[t]emos que respeitar as diferenças, mas precisamos construir a infraestrutura para permitir essas diferenças. Precisamos dos canos e do encanamento para maximizar os fluxos de dados*"[58].

[57] Sigla em inglês para *Information Commissioner's Office*.
[58] INFORMATION COMMISSIONER'S OFFICE. A Bretton Woods for data. Disponível em: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/09/a-bretton-woods-for-data/#:~:text=It%20is%20my%20view%20that,is%20integral%20to%20digital%20innovation.>. Acesso em: 31.05.2022.

Autor

PEDRO GRUEIROS

Mestrando em Direito Civil pela PUC-Rio. Bolsista da Fundação Konrad Adenauer. Advogado. Pesquisador de Direito e Tecnologia no ITS Rio. Integrante do Núcleo Legalite da PUC-Rio. Graduado em Direito pelo Ibmec-RJ.

Editoração e Revisão

CELINA BOTTINO

Graduada em direito pela PUC-Rio, mestre em direitos humanos pela Universidade de Harvard. Especialista em direitos humanos e tecnologia. Foi pesquisadora da Human Rights Watch em Nova York. Supervisora da Clínica de Direitos Humanos da FGV Direito-Rio. Foi consultora da Clínica de Direitos Humanos de Harvard e pesquisadora do ISER. Associada do Centro de Defesa dos Direitos da Criança e Adolescentes do Rio de Janeiro. Atualmente desenvolve pesquisas na área de direitos humanos e tecnologia coordenando projetos na área de liberdade de expressão e privacidade. É afiliada ao Berkman Klein Center de Harvard e diretora de projetos do ITS.

CHRISTIAN PERRONE

Pesquisador Fulbright (Universidade de Georgetown, EUA), Doutor (UERJ) em Direito Internacional e Direito Digital; Mestre - LL.M.- em Direito Internacional (Universidade de Cambridge, Reino Unido); Diplomado em Direito Internacional dos Direitos Humanos pelo Instituto Universitário Europeu (EUI, Itália). Ex-secretário da Comissão Jurídica Interamericana da OEA e especialista em Direitos Humanos da Comissão

Interamericana de Direitos Humanos e da Corte Interamericana de Direitos Humanos. Atualmente, advogado, consultor de Políticas Públicas e Head das áreas de Direito e Tecnologia e GovTech do ITS.

Projeto Gráfico

MARIANA BERTOLUCI

Designer e artista visual, graduada pela Universidade Federal de Mato Grosso do Sul (UFMS). Se motiva por trabalhos que possuam o propósito de transformação, fazendo com que desenvolva habilidades estratégicas que possam somar com a produção de materiais gráficos. Tem interesse pela interseção entre a tecnologia e educação, além de desenvolver pesquisa nos campos de estudos do marketing e webdesign. É designer e pesquisadora sênior na área de mídias do ITS.

Acesse nossas redes

itsrio.org