PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO
FACULDADE DE DIREITO
NÚCLEO DE MONOGRAFIA JURÍDICA

TRABALHO DE CONCLUSÃO DE CURSO

NATAN JAMIL ÂNGELO

ACORDOS BILATERAIS COMO FERRAMENTA DE TRANSFERÊNCIA INTERNACIONAL DE DADOS: uma análise à luz do *Safe Harbor*, *Privacy Shield* e *Data Privacy*.

São Paulo
2023

NATAN JAMIL ÂNGELO

ACORDOS BILATERAIS COMO FERRAMENTA DE TRANSFERÊNCIA INTERNACIONAL DE DADOS: uma análise à luz do Safe Harbor, Privacy Shield e Data Privacy.

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de bacharel em Direito pela Pontifícia Universidade Católica de São Paulo.

Orientadora: Prof. Dra. Clarisse Laupman Ferraz Lima

São Paulo

2023

NATAN JAMIL ÂNGELO

ACORDOS BILATERAIS COMO FERRAMENTA DE TRANSFERÊNCIA INTERNACIONAL DE DADOS: uma análise à luz do Safe Harbor, Privacy Shield e Data Privacy.

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de bacharel em Direito pela Pontifícia Universidade Católica de São Paulo.

São Paulo, 07 de dezembro de 2023

_____

Profª Dra. Clarisse Laupman Ferraz Lima
Pontifícia Universidade Católica de São Paulo

_____

Profª Dra. Maitê Cecília Fabbri Moro
Pontifícia Universidade Católica de São Paulo

AGRADECIMENTOS

O primeiro agradecimento desta Monografia é *in memoriam* à Dona Onesta. Avó amada, divertida, cuidadosa e sonhadora, sempre dizia que gostaria de me ver terminando a graduação, ora, quem não gostaria de ver o primeiro neto a chegar ao ensino superior. Infelizmente, Dona Onesta, com a letra "O" como ela frisava, nos deixou, me deixou na metade da graduação. Sua partida criou um vácuo na minha vida, pois onde mais poderia encontrar aconchego e colo de vó. Os tempos passaram, as feridas fecharam e hoje tenho certeza de que ela acompanhou a minha trajetória aqui, mesmo diante de todos os percalços, segurou a minha mão e me trouxe até aqui. Então, para além de tudo, esta Monografia foi feita para minha avó que tanto queria o primeiro neto no ensino superior.

Não menos importante, dedico esta Monografia aos meus pais que tanto fizeram para que eu pudesse chegar aqui. Flavio e Renata, um serralheiro e uma técnica de enfermagem, fizeram tudo ao seu alcance para que eu pudesse chegar ao ensino superior, sempre estiveram ao meu lado na alegria e na tristeza, mesmo que sentimentalmente contrariados pela minha saída da cidade natal para São Paulo. Esta Monografia também é para vocês que todos os anos se preocupavam com a renovação da bolsa de estudos concedida a mim, que me ligavam todos os dias para saber se tudo estava bem. Vocês são incríveis e me inspiram todos os dias.

Para além dos vínculos familiares, gostaria de agradecer aos amigos e colegas que fiz em virtude da PUC-SP. Um rio-pretense de 18 anos que não conhecia ninguém foi integrado aos grupos sociais graças a vocês. O meu muito obrigado a todos vocês que me proporcionaram os melhores 5 anos da minha vida, vocês são ouro, são alma e são coração.

Por fim, meu último agradecimento irá às pessoas que me fizeram adentrar ao mundo da privacidade e proteção de dados: meu time de Tecnologia do Mattos Filho. Um time com mentes brilhantes e pessoas inspiradoras criaram este profissional que se forma logo mais, criaram um estudante que continuará o caminho em busca da proteção de dados. Aos que discutiram comigo o meu tema de pesquisa, em especial Luiza Mendonça Santos, obrigado por me mostrar o caminho.

"*A privacidade é muito importante para que a deixemos atrofiar. Quem você é e o que você faz não é da conta de ninguém. Você não é um produto a ser transformado em dados e alimentar predadores por um preço. Você não está à venda. Você é um cidadão, e a privacidade lhe é devida. É um direito seu. A privacidade é como vendamos o sistema para que ele nos trate de forma imparcial e justa. É como damos poder aos nossos cidadãos. É como protegemos indivíduos, instituições e sociedades de pressões externas e abusos. É como demarcamos um espaço para nós mesmos no qual podemos relaxar livremente, criar laços com os outros, explorar novas ideias e tomar nossas próprias decisões.*" (CARISSA VÉLIZ)

RESUMO

JAMIL ANGELO, Natan. **Acordos bilaterais como ferramenta de transferência internacional de dados: uma análise à luz do Safe Harbor, Privacy Shield e Data Privacy**. Tese (Graduação em Direito) – Faculdade de Direito da Pontifícia Universidade Católica de São Paulo. São Paulo, 2023.

Resumo: A dinâmica das transferências internacionais de dados impacta diariamente no desenvolvimento econômico e progresso, uma vez que vivemos em uma sociedade da informação que se encontra voraz por novos dados. Mecanismos que buscam facilitar e agilizar processos de adequação às legislações de proteção de dados diversas devem ser perseguidos em um mundo globalizado. Portanto, a análise dos acordos bilaterais firmados entre União Europeia e Estados Unidos da América são relevantes para considerações de como fazer e o que deve conter nos acordos sobre o tema, exatamente pela fundamentação das decisões do Tribunal de Justiça da União Europeia que invalidou os dois primeiros acordos. Como será apresentado a seguir, o sistema brasileiro de proteção de dados está no caminho correto de consonância com o sistema europeu e, inclusive, possui disposições claras acerca da possibilidade das transferências com base em acordos bilaterais. Com preocupações como soberania nacional, os acordos bilaterais são válidos para que transferências sejam efetuadas, sobretudo, caso contenham requisitos mínimos que serão abordados a seguir. O futuro chegou no mundo globalizado e é o momento do Brasil se interpor nas dinâmicas internacionais de proteção de dados e privacidade.

Palavras-chave: acordos bilaterais; transferência internacional; dados pessoais; LGPD.

ABSTRACT

JAMIL ANGELO, Natan. **Bilateral agreements as tool for international data transfer: an analysis in the context of Safe Harbor, Privacy Shield and Data Privacy**. Thesis (Law Degree) – Law School of the Pontifical University Catholic of São Paulo. São Paulo, 2023.

Abstract: The dynamics of international data transfers have an impact on economic development and progress daily, since we live in an information society that is voracious for new data. Mechanisms that seek to facilitate and speed up processes of compliance with various data protection laws must be pursued in a globalized world. That said, the analysis of the bilateral agreements signed between the European Union and the United States of America is relevant to considerations of what to do and what they should contain, precisely because of the reasoning behind the decisions of the Court of Justice of the European Union that invalidated the first two agreements. As will be presented below, the Brazilian data protection system is on the right track in line with the European system and even has clear provisions on the possibility of transfers based on bilateral agreements. With concerns about national sovereignty, bilateral agreements are valid for transfers to take place, especially if they contain minimum requirements, which will be discussed below. The future has arrived in the globalized world and it is time for Brazil to interpose itself in the international dynamics of data protection and privacy.

Keywords: bilateral agreements; international data transfer; personal data; LGPD.

SUMÁRIO

INTRODUÇÃO

O desenvolvimento tecnológico nos últimos anos se mostrou importante para o avanço da sociedade da informação nos mais variados âmbitos: saúde, educação, segurança pública, economia, lazer, transporte e trabalho. A sociedade mundial se maravilhou com as benesses que o progresso poderia trazer, entretanto, rapidamente experimentou as mazelas de uma vida *online*.

Desde 1890, os acadêmicos vêm estudando um tema relevante e que, hoje, mais do que nunca, é muito relevante: a privacidade. O desenvolvimento tecnológico teve influência decisiva como o Direito poderia assegurar a privacidade, a proteção de dados e o direito de ser deixado só. Isto posto, as nações começaram a desenvolver os seus marcos legais relacionados à proteção de dados pessoais na era digital, tendo o Brasil ingressado permanentemente em 2018.

Abordar proteção de dados é também abordar economia e regulação de mercado, considerando que o fluxo transfronteiriço de dados exercerá um maior impacto no crescimento do Produto Interno Bruto (PIB) global do que bens comerciais. Na quarta revolução industrial, os dados pessoais se mostraram como um bem infinito e abundante podendo, por exemplo, vir a ser objeto de transações comerciais. As novas tecnologias agregam valor aos dados pessoais tratados, por isso que sua coleta, armazenamento e transferência são relevantes aspectos mercadológicos para o desenvolvimento econômico.

Sob o enfoque específico das transferências internacionais, esta Monografia se propõe a analisar como os dados pessoais são transferidos e sob qual hipótese legal autorizadora. Além disso, visa-se entender a dinâmica das transferências internacionais que, dentre outras coisas, sujeitam os dados pessoais coletados a não estarem no território nacional até no mesmo momento da coleta.

O objetivo precípuo é analisar, sob o enfoque das transferências internacionais, como mecanismos alternativos conseguem respaldar este tipo de tratamento de dados. A intenção é, na verdade, entender como acordos bilaterais são mecanismos eficientes e ágeis que podem justificar uma transferência internacional sem, portanto, deixar a privacidade e proteção de dados de lado. Por isso, esta Monografia analisará três acordos bilaterais firmados entre União Europeia e Estados Unidos da América: *Safe Harbor Agreement*, *Privacy Shield* e *Data Privacy Framework*.

Por fim, o resultado esperado é uma análise sobre como acordos bilaterais poderiam ser comportados no ordenamento jurídico brasileiro e, para além disso, como um conteúdo mínimo poderia ser esperado, a partir das experiências estadunidenses e europeias de invalidação de seus dois primeiros acordos sobre transferência internacional de dados. Ainda no mesmo sentido, se abordará como uma proposta viabilizada pelo Mercado Comum do Sul (MERCOSUL) pode ser útil.

Para que tudo isso aconteça, o método de pesquisa será composto por uma metodologia de abordagem e uma de procedimento. A metodologia de abordagem se dará pelo método indutivo, ou seja, partir-se-á de dados particulares relacionados aos acordos bilaterais firmados no âmbito da U.E., bem como das decisões que decretaram sua invalidade para, por fim, chegar aos termos gerais positivos e negativos de como transferências internacionais de dados poderiam ser validadas. Posteriormente, a análise será incluída nos moldes brasileiros à luz da LGPD.

O método de procedimento será comparativo entre os acordos firmados pela U.E. e E.U.A. com a legislação brasileira. Portanto, visa-se analisar, comparativamente, os motivos que deram ensejo aos acordos bilaterais, bem como os motivos que levaram a sua inadequação para, assim, trazer uma análise no âmbito brasileiro em conformidade com a LGPD.

Portanto, a primeira Seção propõe-se a inserir um panorama geral sobre como as demandas de proteção de dados e as transferências internacionais foram surgindo com passar dos tempos. Não somente, mas propõe-se a abordar como diferentes culturas de proteção de dados surgiram com o desenvolvimento da sociedade, em especial, a estadunidense, a europeia e a brasileira. Ainda, será abordado especificamente como a legislação brasileira abordou o tema e quais perspectivas são esperadas para o futuro.

Na segunda Seção serão abordados os acordos bilaterais firmados entre UE e EUA, bem como o conteúdo e mecanismos gerais utilizados em sua entabulação. A partir disso, uma análise será feita das decisões exaradas pelo Tribunal de Justiça da União Europeia (TJUE) que levou a invalidação dos dois primeiros acordos entre as partes, a fim de entender os motivos que fundamentaram tal decisão.

Na terceira e última Seção, o intuito é expor como seria cabível um acordo bilateral na legislação brasileira e, ainda, como a Lei Geral de Proteção de Dados previu mecanismos como estes para autorizarem as transferências internacionais. A partir disso, visa-se demonstrar, a partir dos fundamentos do TJUE, o que poderia ser

um acordo de balizaria interesses de soberania nacional e proteção de dados e à privacidade. Em seguida, será abordado como o Mercosul vem se tornando um importante bloco econômico que pode estar a frente da criação da maior zona de livre de comércio, inclusive, de dados pessoais, no mundo.

1. TRANSFERÊNCIA INTERNACIONAL DE DADOS

Esta Seção será responsável por delimitar o escopo das transferências internacionais de dados, a fim de entender sua relação histórico-evolutiva com a dinâmica do livre fluxo de dados. Visa-se delinear mínimos conceitos que interceptam as transferências internacionais de dados pessoais e trazem à baila o aspecto econômico de sua regulação. Por fim, instiga-se a construção de um raciocínio lógico-jurídico das hipóteses legais que autorizam transferências internacionais na LGPD para, assim, criar uma base sólida para alcançar o objetivo desta Monografia.

1.1. BREVE CONTEXTUALIZAÇÃO DA EVOLUÇÃO REGULATÓRIA DA PROTEÇÃO DE DADOS NA UE, EUA E BRASIL

O avanço da sociedade se mostrou incessante e, nas últimas décadas, cada vez mais rápido, sendo fruto de uma globalização latente entre a comunidade internacional desde a Primeira Revolução Industrial. Após o decurso de séculos, o mundo passou por inúmeras mudanças, antes com um êxodo rural e início do processo de industrialização, passando por um desenvolvimento tecnológico-industrial e o descobrimento de novas fontes de energia, chegando ao cerne do que move a Indústria 4.0 hoje: tecnologia, dados e inovação. (ERNST; FRISCHE, 2015, p. 8-9)

Do avanço industrial pôde-se perceber uma mudança drástica na economia mundial decorrente da transposição do valor dos bens de consumo e serviço. Para a economia brasileira, o pau-brasil, ouro e diamante tiveram seu papel importante no desenvolvimento extrativista. Em seguida, o café desempenhou com maestria a ascensão de uma elite concentrada no sudeste brasileiro, e, mais recentemente, a descoberta do pré-sal colocou o Brasil no mapa do petróleo como um importante produtor. Essa linha cronológica faz parte do acompanhamento das terras tupiniquins à ordem mundial.

A sociedade mundial, mordaz pelo avanço e progresso tecnológico, desenvolveu-se a ponto de conhecer um novo bem infinito, abundante e dinâmico: seus próprios dados. Para enfatizar a mudança de paradigmas, pesquisadoras da

Nebraska University citam Michael Palmer[1], o responsável por difundir o termo mais relevante para a próxima era, em comentários sobre a palestra de Clive Humby na *Kellogg School* em 2006: dados são o novo petróleo. (SRIVASTAVA; SINGH; SONKAR, 2021, p. 2 apud PALMER, 2006)

Com a mudança nas dinâmicas mundiais de transposição de valores ao novo petróleo, verificou-se um movimento internacional, inicialmente, centralizado nos países europeus, de proteção aos dados pessoais dos cidadãos e o reconhecimento da privacidade como direito fundamental[2]. O primeiro relato do início da discussão sobre proteção de dados pessoais se deu em 1890, quando dois advogados americanos, Samuel D. Warren e Louis Brandeis, escreveram um artigo denominado "O direito à privacidade"[3], onde argumentavam sobre o direito de ser deixado sozinho, sendo essa a definição de privacidade para os autores. (BRANDEIS; WARREN, 1890, tradução nossa)

A partir disso, o mundo se moveu em inúmeras tentativas para proteger os dados pessoais da população, sendo um marco especial a adoção da Convenção nº 108 de 1981 no âmbito do Conselho da Europa (Convenção 108), que era destinada à proteção de dados pessoais em tratamentos automatizados. A regulamentação do compartilhamento de dados entre os países do Conselho da Europa era o caminho adequado para a criação de uma unidade entre os países membros da UE, considerando o crescente fluxo de transfronteiriço de dados pessoais há época e a conciliação entre o direito à privacidade e o livre fluxo de dados. (CONSELHO DA EUROPA, 1981, tradução nossa)[4]

Com esforço, o Parlamento e o Conselho da União Europeia nas décadas seguintes foram responsáveis pela adoção de outras regulamentações, ressalta-se a criação da Diretiva Europeia de Proteção de Dados em 1995 (Diretiva 95/46/CE) e a sua revogação pelo recente Regulamento Geral de Proteção de Dados em 2016

---

[1] PALMER, Michael. **ANA Marketing Maestros: Data is the New Oil**. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

[2] O reconhecimento do direito fundamental à privacidade se deu na Declaração Universal de Direitos Humanos em 1948, em especial em seu Artigo 12º, conforme segue: "Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei." (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948)

[3] No original: "The Right to Privacy."

[4] No original: "Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms; [...] Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples"

(RGPD), que entraria em vigor em 25 de maio de 2018. Tendo sempre como base o marco legal da proteção de dados como um direito fundamental de seus cidadãos, conforme ensina Muchiuti (2022, p. 22):

> O RGPD tem um caráter bastante protetivo quanto ao tratamento de dados pessoais, já que direito à privacidade é um direito fundamental sob a perspectiva da Carta dos Direitos Fundamentais da UE (UE, 2000, art. 7º e 8º), diploma legal que reúne formalmente em um único documento os direitos humanos tutelados pela UE e os países que a integram.

Enquanto o continente europeu passava por uma regulação relacionada à privacidade e proteção de dados pessoais baseado no direito fundamental dos seus cidadãos, os Estados Unidos da América (EUA), com características inerentes de seu federalismo, criaram um marco legal de regulações nacionais, estaduais e municipais relacionadas à proteção de dados. O exemplo claro desse fenômeno estadunidense é o crescimento exponencial das regulações estaduais como a Lei de Privacidade do Consumidor da California (CCPA) emendada pela Lei de Direitos de Privacidade da Califórnia (CPRA), a Lei de Privacidade do Colorado (CPA), a Lei de Privacidade de Dados de Connecticut (CTDPA), a Lei de Privacidade do Consumidor de Utah (UCPA), e a Lei de Proteção de Dados do Consumidor da Virgínia (VCDPA).

Em que pese a atuação estadual nos EUA, os estadunidenses deram um passo importante numa legislação federal de proteção de dados em 2022: a Lei Federal Americana de Privacidade e Proteção de Dados (ADPPA). Aprovada pelo Comitê de Energia e Comércio da Câmara dos Representantes dos EUA, a ADPPA possui o objetivo de "fornecer aos consumidores direitos fundamentais de privacidade de dados, criar fortes mecanismos de supervisão e estabelecer uma aplicação significativa." (ESTADOS UNIDOS DA AMÉRICA, 2022, p. 1, tradução nossa)[5], com um aspecto setorial, diferentemente da UE, os EUA avançam na regulação da proteção de dados e privacidade.

O sul global, por sua vez, desempenhou um movimento parecido com a UE, inclusive no conteúdo de suas legislações nacionais, prezando por mecanismos, definições e princípios que se alinham com o RGPD. Essa influência da UE nos padrões regulatórios mundiais foi estudada pela Prof.ª Anu Bradford da *Columbia University*, ela argumenta que, mesmo diante de uma crise institucional, Brexit e

[5] No original: "*To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement.*".

crescimento desacelerado, o velho continente ainda é capaz de influenciar a dinâmica mundial e moldar o sistema econômico global, a partir de uma regulamentação unilateral. (BRADFORD, 2016, p. 5)

Por sua vez, o Brasil, sob o comando da Pres. Dilma Rousseff em 2013, ao descobrir o escândalo divulgado por um ex-consultor estadunidense da Agência de Segurança Nacional (NSA), que envolvia a espionagem online pelo governo estadunidense de sua população e de outras nações, incluindo o Brasil[6], promulgou a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet – MCI). O MCI foi elogiado mundialmente, sendo a primeira lei brasileira que estabeleceu direitos e deveres para usuários e provedores de internet no país. (PELEGRINI; PELEGRINI, 2014, p. 267)

O MCI possui como objetivo principal disciplinar o uso da internet no Brasil, além disso, a legislação é responsável por perseguir alguns outros propósitos estampados em seu Art. 4º, como: o direito de acesso à internet a todos os brasileiros; o acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; a inovação e o fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e a adesão a padrões tecnológicos abertos que permitam a comunicação, acessibilidade e interoperabilidade entre aplicações e bases de dados. (BRASIL, 2014)

Temas relacionados à neutralidade de rede, não suspensão da conexão à internet, privacidade, segurança no registro de conexão dos usuários, garantia da liberdade de expressão e proteção dos dados pessoais, foram consagrados como princípios do MCI. A referida legislação foi responsável por trazer à baila os primeiros conceitos, princípios e diretrizes que seriam necessários para a promoção de padrões abertos para a internet com a finalidade de minimizar tentativas que prejudiquem ou onerem o livre acesso à informação. (JESUS; OLIVEIRA, 2014, p. 25)

Em uma guinada no assunto de proteção de dados em todo o mundo e com base no “Efeito Bruxelas”, o Brasil se comprometeu a regular a proteção de dados em seu território. Dessa forma, a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados – LGPD) surgiu, tendo sido utilizado como texto base um antigo documento publicado em 30 de novembro de 2010 pelo Ministério da Justiça,

---

[6] G1. **Dilma sanciona o Marco Civil da internet na abertura da NETMundial**. Disponível em: https://g1.globo.com/tecnologia/noticia/2014/04/netmundial-inicia-com-obrigado-snowden-e-defesa-da-internet-livre.html. Acesso em: 25 jun. 2023.

documento este que foi responsável por tornar público o debate. (DONEDA, 2021, p. 35).

Passados alguns anos após o debate público em torno da possibilidade da regulamentação à proteção dos dados pessoais no Brasil, o anteprojeto de lei, após inúmeras discussões, foi tornado público pela Secretaria Nacional do Consumidor (SENACON) que realizou uma nova rodada de contribuições. Finalmente, em 13 de maio de 2016, o projeto de lei foi encaminhado à Câmara dos Deputados sob o PL nº 5.276/2016. (DONEDA, 2021, p. 36)

Como era de se esperar, o debate em torno da proteção de dados no Brasil, nas palavras de Danilo Doneda (2021, p. 36), "já havia ecoado na sociedade a ponto de haver outros projetos de lei sobre o tema em tramitação" ao mesmo tempo que o PL nº 5.276/2016[7]. Em que pese o encaminhamento desse PL na Câmara dos Deputados, outros projetos de lei estavam em ritmo mais avançado, sendo que eles foram apensados ao PLC nº 53/2014 que, à época, acabara de ser aprovado na Câmara dos Deputados e, após um requerimento de urgência na tramitação no Senado Federal, foi aprovado e encaminhado para sanção presidencial em 5 de julho de 2018.

Após a corrida legislativa para se aprovar uma legislação de proteção de dados no Brasil, o referido projeto de lei foi promulgado em 14 de agosto de 2018 com vetos. Nesse sentido, ensina Danilo Doneda (2021, p. 36):

> Sua sanção, no entanto, foi acompanhada de vetos a alguns de seus dispositivos, inclusive da integralidade daqueles referentes à Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados e Privacidade. Posteriormente, foi editada a Medida Provisória 869/2018, que veio a se tornar a Lei 13.853/2019 que, além de modificar a LGPD em diversos pontos, finalmente definiu as características da ANPD e do seu Conselho, de acordo com os arts. 55-A a 55-L da LGPD. Outra das modificações foi a extensão de sua *vacatio legis*, que passou de fevereiro de 2020 para agosto de 2020, com exceção dos referidos artigos sobre a ANPD e Conselho Nacional de Proteção de Dados e da Privacidade, cuja vigência é imediata.

Com um processo truncado de edições de medidas provisórias, alteração do período de *vacatio legis* para alguns dispositivos, a promulgação da LGPD representou um marco na comunidade acadêmica que se debruçou, durante anos, no

[7] Naquele momento, o Congresso Nacional contava com inúmeras iniciativas para proteção de dados no Brasil, dentre elas: PL nº 4.060/2012, PLS nº 330/2013, PLS nº 131/2014, PLS nº 181/2014 e PLC nº 53/2018.

estudo da proteção de dados. A LGPD foi responsável por sistematizar a estrutura robusta de proteção de dados que existe hoje no Brasil, a partir de elementos anteriores contidos no ordenamento jurídico e com a inserção de outros, ela causou um impacto normatizando a matéria de forma geral. (DONEDA, 2021, p. 37)

A LGPD tomou o seu lugar e ganhou espaço nos debates públicos e acadêmicos, a partir dela se criou a inserção de uma gama de institutos jurídicos próprios, princípios, direitos dos titulares, balanceamento entre a tutela dos titulares de dados frente às medidas tomadas pelos agentes de tratamento, dentre outras. (DONEDA, 2021, p. 37). O Art. 2º da LGPD foi precursor dos fundamentos do tratamento de dados pessoais no Brasil, dentre eles: a privacidade; a autodeterminação informativa; a liberdade de expressão e seus consectários; a inviolabilidade da intimidade; a desenvolvimento da personalidade e exercício da cidadania; a dignidade da pessoa humana; o desenvolvimento econômico; a livre iniciativa; e, por fim, mas não menos importante, os direitos humanos. (BRASIL, 2018)

A partir disso, o debate em torno do tema de proteção de dados foi avassalador, a ponto da Emenda Constitucional nº 115 de 10 de fevereiro de 2022, alterar a Constituição Federal (CRFB) para acrescer o direito à proteção dos dados pessoais como um direito fundamental, adicionando, assim, o Art. 5º, LXXIX, à CRFB. A mesma Emenda Constitucional incluiu outros dois incisos, nos Arts. 21 e 22 da CRFB, para dar competência privativa de legislar sobre proteção e tratamento de dados pessoais e atribuir a responsabilidade de organizar e fiscalizar a proteção e o tratamento de dados pessoais à União. (BRASIL, 1988)

Dada esta breve e resumida contextualização da evolução das legislações de proteção de dados na UE, EUA e Brasil, o tema desta Monografia se perpassa por um dos aspectos mais relevantes, ao menos para o Brasil e UE, para qualquer legislação de proteção de dados: transferência internacional de dados pessoais. As Subseções seguintes se propõem a explicar os mecanismos e hipóteses previstas nas legislações aplicáveis sobre transferência internacional de dados.

1.2. DINÂMICA DAS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS NO MUNDO

Numa realidade analógica, o significado de transferência de dados poderia ser facilmente identificado como a junção de vários documentos e seu envio a outro

lugar. Do ponto de vista internacional, o conceito é replicado, apenas sendo diferenciado pelo destino daqueles documentos. O conceito de transferir dados internacionalmente, frise-se, em uma realidade analógica, parte do pressuposto de que o seu envio cruze as fronteiras físicas em seu sentido amplo, ou seja, modifique a jurisdição em que aquela transferência está submetida. (MARQUES; AQUINO, 2021, p. 310)

Atualmente, o referido conceito é insuficiente para delinear as complexidades que abarcam uma transferência internacional de dados no mundo digital. O exercício de imaginar que um dado é criado e para ser transferido internacionalmente existe uma rota predeterminada pouco encontra relação com a realidade digital. Isto pois, conforme explica Marques e Aquino (2021, p. 310) “considerando as formas e os modelos em que os dados podem ser tratados hoje em dia, mais precisa é a noção de que os dados podem já não estar mais dentro dos limites do Estado no mesmo instante em que são criados”.

O que se tem, atualmente, é uma dificuldade de analisar as dinâmicas que delimitam o escopo de uma atividade de tratamento que envolva transferência internacional de dados, bem como a visualização clara do instante em que isso acontece. A distinção entre o momento de coleta, compartilhamento, transferência e armazenamento é complexa e demanda uma abstração para fins de aplicação de uma jurisdição ou outra.

Além das perspectivas relacionadas à complexidade das transferências internacionais de dados, uma importante consideração deve ser delineada sobre as regulações que transpassam o tema: regular transferência internacional de dados é também regular mercado. As regulamentações destinadas às transferências internacionais possuem um caráter comercial, a depender do país, mais protecionista ou menos. Em consonância com o exposto anteriormente, se os dados são o novo petróleo, o seu livre fluxo pode trazer aspectos relacionados às barreiras do comércio e demais transações. (MARQUES; AQUINO, 2021, p. 311)

Exatamente pela existência da correlação entre mercado e transferência internacional de dados é que podem existir distorções regulatórias que influenciam a atração de diferentes empresas e negócios para cada país. (SANTOS; VERONESE, 2021, p. 95) Os modelos regulatórios mais flexíveis tendem a proporcionar um campo de investimento mais favorável às empresas de tecnologia ou que utilizam em seu *core business* o tratamento de dados pessoais, excetuado casos em que, mesmo

diante de um modelo rígido, a transferência de dados para aquele lugar é necessária por questões de mercado consumidor, como é o caso da UE.

Portanto, as transferências internacionais de dados vão muito além de uma relação entre agentes de tratamento e titulares de dados, mas também adentram nas relações comerciais e o livre fluxo de produtos e serviços. Nesse sentido, James Manyika (2016, p. 36, tradução nossa) na coordenação do artigo sobre globalização digital publicado pelo *McKinsey Global Institute*, afirma que:

> Os fluxos de dados - tanto dentro dos países quanto entre eles - refletem as atividades de indivíduos e empresas. Muitas pessoas presumem que a Internet é dominada por indivíduos que assistem ao YouTube e a outros vídeos de streaming, trocam e-mails e fazem publicações nas mídias sociais. Mas uma grande parte do tráfego da Internet também é conduzida por empresas que interagem com suas operações, fornecedores e clientes estrangeiros. O aspecto comercial dos fluxos de dados provavelmente assumirá uma dimensão mais profunda em um futuro próximo, à medida que mais empresas incorporarem monitores, sensores e dispositivos de rastreamento em seus ativos físicos.[8]

A fim de acomodar uma resolução harmônica e, por vezes, inibir ações anticoncorrenciais, os Estados se propuseram a eleger padrões regulatórios internacionais que convergissem entre si para, nas palavras de Marques e Aquino (2021, p. 311), “evitar que justificativas regulatórias fundadas na privacidade e proteção dos dados pessoais pudessem dar causa a barreiras ao comércio e às demais transações internacionais”. Por isso, o “Efeito Bruxelas” possui grande influência no tema sobre transferência internacional de dados, o velho continente ainda se coloca como um pivô regulatório que, por muitas vezes, se mostra restritivo no tocante à privacidade.

Na tentativa de harmonizar os diferentes modelos regulatórios mundiais e reduzir o impacto das fronteiras nacionais, Kuner sugere que existem diversos mecanismos que podem ser implementados para a harmonização de diferentes sistemas jurídicos, como por meio de tratado ou convenção multilateral ou bilateral; um modelo ou lei uniforme que os Estados podem incorporar em sua legislação nacional; uma codificação de costumes e usos promulgada por uma organização não-

[8] No original: “Data flows—both within countries and between them—reflect the activities of individuals and of businesses. Many people assume that the Internet is dominated by individuals viewing YouTube and other streaming videos, trading e-mails, and posting on social media. But a large share of Internet traffic is also driven by companies interacting with their foreign operations, suppliers, and customers. The business aspect of data flows is likely to take on a deeper dimension in the near future as more companies embed monitors, sensors, and tracking devices into their physical assets.”

governamental; termos e condições que podem ser incorporados em contratos e outros documentos celebrados entre particulares; e dentre outros. (KUNER, 2009, p. 12)

Por isso, foram criados *frameworks* macro legais baseados na concordância de padrões para proteção de dados pessoais. À título exemplificativo cita-se a Convenção 108 do Conselho da Europa, as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais (Diretrizes de 1980) da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), a APEC *Privacy Framework* de 2005, dentre outras.

Neste sentido, a UE, ainda na Convenção 108, percebeu que o fluxo de dados pessoais tinha um caráter eminentemente econômico e, por isso, deveria ser livre em seu mercado interno com a circulação livre de mercadorias, pessoas, serviços e capital. No âmbito internacional, a UE atuou na propagação de ferramentas que possibilitassem que o fluxo de dados entre países fosse tão livre quanto em seu interior, assim, dando ensejo a regulações sobre transferência internacional de dados e acordos bilaterais que as viabilizasse. (GARCÍA-CUEVAS ROQUE, 2014, p. 173)

Ao balizarmos os fatores que determinam a regulação das transferências internacionais de dados pessoais temos duas situações que se colocam no atual estágio de desenvolvimento global, expansionista e capitalista. De um lado, preocupações legítimas que justificam a regulação do tema em prol de uma sociedade livre com direito à proteção de seus dados e autodeterminação informativa; de outro lado, o justo direito de as empresas não estarem adstritas às jurisdições nacionais que possam restringir a expansão de suas atividades e o fornecimento de produtos e serviços. (MARQUES; AQUINO, 2021, p. 312)

A necessidade de uma regulação pluralista cresce na medida que o processo de globalização é intensificado com o passar dos anos, sendo necessário que os Estados atuem de forma consentânea na prospecção de um interesse em comum que, neste caso, é garantir o direito à privacidade e proteção de dados dos titulares e operacionalizar o funcionamento das empresas de economia globalizada. Esta hipótese permeia o tema desta Monografia, como os Estados tentaram viabilizar as transferências internacionais de dados, equalizando as justas expectativas da sociedade e setores empresariais.

Isto posto, a análise das hipóteses que autorizam as transferências internacionais de dados pessoais na legislação brasileira é o próximo passo para

entender as ferramentas que existem hoje e, com base na experiência internacional, visualizar a extensão de tais mecanismos.

1.3. TRANSFERÊNCIA INTERNACIONAL DE DADOS NA LGPD

Antes de adentrar aos mecanismos previstos na LGPD que legitimam uma transferência internacional de dados, bem como analisar a sua correspondência com o RGPD, precisa-se criar uma base clara dos termos e conceitos que são introduzidos ao sistema jurídico brasileiro a partir do advento da LGPD. Isto posto, para uma maior compreensão sobre o tema, a próxima Subseção se proporá a explicar, com base na LGPD, as conceituações necessárias para a explanação do assunto.

1.3.1. Conceitos relevantes da LGPD

O Art. 5º da LGPD é o dispositivo legal capaz de trazer as explicações necessárias para entender todos os novos conceitos jurídicos que permeiam a proteção de dados no Brasil e foram incluídos com a sua aprovação. Como dito anteriormente, a LGPD trouxe novos institutos jurídicos e conceitos que merecem sua explanação, nas palavras de Danilo Doneda (2021, p. 37):

> [...] a lei apresenta diversos elementos novos que, por si sós, causaram impacto, e o fato de consolidarem a matéria em uma normativa geral foi somente o primeiro deles: com a LGPD, passam a integrar o ordenamento toda uma nova série de institutos próprios da disciplina da proteção de dados, como conceitos e institutos próprios [...].

A primeira explicação necessária gira em torno da própria importância da delimitação sobre a aplicabilidade da LGPD, ou seja, o que um dado pessoal. Conforme, o Art. 5º, I, o dado pessoal é todo e qualquer “informação relacionada a pessoa natural identificada ou identificável”. (BRASIL, 2018). Assim, a LGPD se aplicará não somente àqueles dados diretos que identifiquem um individuo (e.g. nome, RG, CPF), mas também àqueles que podem, a depender da circunstância, identificar uma pessoa (e.g. geolocalização), sendo que este indivíduo é conceituado como o titular dos dados pessoais. (TEIXEIRA; GUERREIRO, 2022, p. 17)

Por definição, o dado pessoal refere-se a uma pessoa natural e não se aplica às pessoas jurídicas, entretanto, este conceito não foi suficiente para delimitar a

complexidade dos dados pessoais. A LGPD, no seu Art. 5º, II, traz uma espécie de dado pessoal que se refere à sensibilidade daquela informação, ou seja, dados que envolvam "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" são classificados como dados pessoais sensíveis. (BRASIL, 2018)

O dado pessoal sensível é diferenciado do dado pessoal – que chamaremos à título didático de comum –, exatamente pela sua capacidade de discriminar pessoas naturais. A tutela jurídica da LGPD ao dado pessoal sensível será mais rígida em decorrência do intrínseco conteúdo deste tipo de dado pessoal. (TEIXEIRA; GUERREIRO, 2022, p. 17). A proteção jurídica será ferrenha àqueles dados que são potencialmente mais capazes de prejudicar as liberdades e garantias individuais das pessoas naturais, tendo o seu tratamento restrito[9].

Nessa mesma seara, toda e qualquer operação – exemplificativamente "a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (BRASIL, 2018) – que envolva dados pessoais, é considerada um tratamento e será alcançado pelos direitos e obrigações previstos na LGPD. (TEIXEIRA; GUERREIRO, 2022, p. 18)

Do outro lado da baia, temos os agentes que tratam os dados pessoais, sendo que, para fins da LGPD, existem dois: controlador e operador. Conforme o Art. 5º, VI e VII, da LGPD, o controlador e o operador são pessoas naturais ou jurídicas, de direito público ou privado, que se diferenciam pelo mando em relação aos dados pessoais tratados. O controlador é aquele que vai decidir sobre a forma como os dados pessoais serão tratados, por outro lado, o operador é aquele que irá tratar dados pessoais, mas conforme e nas estritas ordens do controlador. (BRASIL, 2018)

E, finalmente, a LGPD define em seu Art. 5º, XV, o conceito de transferência internacional, sendo "a transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro". Importante ressaltar, a LGPD

[9] Os dados pessoais sensíveis possuem algumas restrições (ao serem comparados com os dados pessoais comuns) em seu tratamento, por exemplo, há uma supressão das bases legais que legitima o seu tratamento. Com base no Art. 11, da LGPD, há supressão das bases legais do legítimo interesse, execução contratual e proteção ao crédito. (BRASIL, 2018)

não limita o conceito de transferência internacional de dados apenas ao envio de dados pessoais a outro país, podendo-se considerar como transferência internacional de dados o armazenamento fora do país (e.g. *cloud*) e o acesso remoto aos dados a partir do exterior[10]. (LEONARDI, 2021, p. 300).

Por fim, cumpre ressaltar a definição de autoridade nacional contida no Art. 5º, XIX, sendo mais conhecida como Autoridade Nacional de Proteção de Dados (ANPD), é "órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.". Similarmente às *Data Protection Authorities* (DPAs) no âmbito europeu, a ANPD possui inúmeras atribuições que visam fiscalizar, difundir e regular as práticas de proteção de dados no país.

Dentre as competências da ANPD, há a responsabilidade por emitir decisões de adequação e procedimentos relacionados às transferências internacionais de dados pessoais, tais como a aprovação de cláusulas contratuais padrões (as famigeradas *Standard Contractual Clauses* – SCCs) e normas corporativas globais (*Binding Corporate Rules* – BCRs), conforme se extrai do Art. 35, caput, da LGPD. (LEONARDI, 2021, p. 301).

Isto posto, os conceitos delineados acima serão necessários para compreender, com maior clareza, a dinâmica dos mecanismos previstos na LGPD para concretização das transferências internacionais de dados pessoais. A base conceitual trazida pela LGPD encontra certa relação com o RGPD, por exemplo, trazendo um rol taxativo, e não meramente exemplificativo, do que são dados sensíveis ou até suas considerações do que é considerada uma transferência internacional.

1.3.2. Hipóteses legais de transferência internacional de dados

[10] Para fins comparativos, o European Data Protection Board (EDPB), entidade responsável por garantir o cumprimento do RGPD e promover a cooperação entre as autoridades de proteção de dados dos países da UE, afirma que o acesso remoto ou o armazenamento em nuvem (i.e. cloud) é considerado transferência internacional de dados pessoais. Nestes termos: "É preciso ter em mente que o acesso remoto a partir de um país terceiro (por exemplo, em situações de assistência) e/ou o armazenamento numa nuvem situada fora do EEE, é igualmente considerado uma transferência.". Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_pt.pdf. Acesso em: 12 jul. 2023.
No mesmo sentido, o acórdão do Tribunal de Justiça da União Europeia no Processo nº C-311/18 (caso Data Protection Commissioner vs. Facebook Ireland Ltd and Maximillian Schrems), possui as mesmas considerações acerca das transferências internacionais de dados pessoais. Disponível em: https://curia.europa.eu/juris/document/document.jsf;jsessionid=7904CEA3E6C21F2099A9057EA4DA8623?text=&docid=228677&pageIndex=0&doclang=pt&mode=lst&dir=&occ=first&part=1&cid=611547. Acesso em: 12 ju. 2023.

A LGPD prevê nove hipóteses legais que permitem as transferências internacionais de dados, tais como:

> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
> a) cláusulas contratuais específicas para determinada transferência;
> b) cláusulas-padrão contratuais;
> c) normas corporativas globais;
> d) selos, certificados e códigos de conduta regularmente emitidos;
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> V - quando a autoridade nacional autorizar a transferência;
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. (BRASIL, 2018)

Antes de adentrar às especificidades que autorizam as transferências na LGPD, faz-se necessário esclarecer a principal diferença entre o regime de transferências no Brasil e na UE. Apesar da forte influência do RGPD na elaboração do Art. 33, da LGPD, os diplomas legais se diferenciam no tocante à subordinação das hipóteses legais umas as outras e a sua clara hierarquização.

Para a legislação europeia o primeiro passo é obter uma decisão de adequação entre a UE e o terceiro avaliado, a fim de garantir o mesmo nível de proteção aos dados pessoais que o RGPD e assegurar o livre fluxo de dados (Art. 45(1), do RGPD)[11]. Na ausência de uma decisão de adequação, o segundo passo é garantir que o exportador dos dados adote salvaguardas adicionais, como a utilização

[11] No original: "(1) A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation."

de BCRs ou SCCS (Art. 46(1), do RGPD)[12]. Por fim, na ausência de uma adequação ou salvaguarda adicional, o exportador dos dados só poderá transferi-los com base nas hipóteses excepcionais.[13] (MARQUES; AQUINO, 2021, p. 323)

No RGPD, as hipóteses legais de transferências internacionais estão subordinadas, isto é, devem seguir uma linha hierárquica para que as transferências sejam consideradas válidas. De maneira contrária, a LGPD, a partir de uma interpretação lógica, não dispõe de uma subordinação entre suas hipóteses legais, assim, nas palavras de Marques e Aquino (2021, p. 324):

> Uma leitura de seu texto demonstra que as hipóteses legais foram dispostas igualmente em incisos, sem nenhuma redação estabelecendo causas de subordinação entre as autorizações. Assim, caso não haja decisão de adequação, poderia o controlador optar igualmente pelas demais hipóteses autorizadoras da transferência.

Portanto, as hipóteses legais previstas na LGPD atuam independentemente, sem a necessidade de obter uma em preferência às outras, obviamente, até alguma interpretação da ANPD sobre o tema. Dessa forma, o agente de tratamento poderá transferir internacionalmente dados pessoais com base em alguma das nove hipóteses legais. Por isso, as próximas Subseções se destinam a explicar cada uma das hipóteses, sendo que, por motivos didáticos, as divisões serão três: (i) decisão de adequação; (ii) garantias suficientes; e (iii) exceções legais.

1.3.2.1. Decisão de adequação

A primeira hipótese legal de transferência internacional está relacionada com o grau de adequação na proteção de dados de um país ou organismo internacional quando comparado com o Brasil, conforme o Art. 33, I, da LGPD. Esta hipótese será a mais relevante e amplamente estudada, uma vez que é a partir dela que os acordos bilaterais entre UE e EUA foram entabulados para viabilizar transferências internacionais.

---

[12] No original: “(1) In the absence of a decision pursuant to Article 45(3), a controller or processor may transfer personal data to a third country or an international organisation only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.”

[13] No original: “(1) In the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions [...]”

O procedimento da decisão de adequação está genericamente delineado na LGPD. O Art. 34, da LGPD, expõe sobre a competência da ANPD para avaliar o nível de proteção de dados do país estrangeiro ou organismo internacional, sendo que ela deverá levar em consideração em sua análise: (i) as normas gerais e setoriais em vigor no país ou organismo internacional; (ii) a natureza dos dados; (iii) a observância de princípios gerais de proteção de dados e direitos dos titulares; (iv) a adoção de medidas de segurança; (v) a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados; e (vi) outras circunstâncias específicas que forem relevantes para a transferência. (BRASIL, 2018)

No caso da declaração de adequação do país estrangeiro ou organismo internacional, o fluxo de dados pessoais se daria de forma livre, sem qualquer necessidade da adoção de outros mecanismos para validar a transferência internacional. Portanto, os agentes de tratamento, sem a necessidade de anuência da ANPD ou dos titulares de dados, poderiam transferir os dados internacionalmente para um país ou organismo internacional já devidamente validado e adequado à legislação brasileira. (LEONARDI, 2021, p. 303)

Para além da competência de ANPD em declarar um país ou organismo internacional adequado ao regime de proteção de dados brasileiro, a LGPD prevê os legitimados ativos para requisitarem o processo de análise da adequação. O parágrafo único, do Art. 33, da LGPD, prevê que as pessoas jurídicas de direito público subordinadas à Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI) são as legitimadas a requisitarem tal análise. (BRASIL, 2018)

Em uma breve análise do parágrafo único, incisos I e II, do Art. 1º, da LAI, vê-se que os legitimados são:

> I - os órgãos públicos integrantes da administração direta dos Poderes Executivo, Legislativo, incluindo as Cortes de Contas, e Judiciário e do Ministério Público;
> II - as autarquias, as fundações públicas, as empresas públicas, as sociedades de economia mista e demais entidades controladas direta ou indiretamente pela União, Estados, Distrito Federal e Municípios. (BRASIL, 2011)

Em que pese o conteúdo delimitado pela LGPD, a ANPD ainda não publicou esclarecimentos necessários para o Capítulo V que trata sobre transferência internacional de dados. Entretanto, conforme inserido na Portaria ANPD nº 35, de 4 de novembro de 2022 que trata sobre a agenda regulatória para o biênio de 2023-

2024 (Portaria nº 35/2022), a regulação do tema de transferência internacional está priorizada como Fase 1, sendo possível esperar um posicionamento da ANPD o quanto antes. (BRASIL, 2022)

Por ora, na falta de uma regulação oficial, em que pese a publicação da Consulta Pública nº 2/2023, vislumbra-se que sua regulação vá ao encontro da experiência europeia, devido a sua influência na elaboração da LGPD. Dessa forma, pode-se aguardar que a ANPD utilize alguns mecanismos já delineados pelo *European Data Protection Board* (EDPB), como, por exemplo, considerar que o termo "nível adequado de proteção" não diz respeito à garantia de nível de proteção idêntico, mas "substancialmente equivalente"[14]. (LEONARDI, 2021, p. 303)

A problemática resta ao passo que a ANPD ainda se encaminha para uma regulação sobre as decisões que consideram países ou organismos internacionais adequados à legislação de proteção de dados no Brasil. Como fica evidente, a tarefa é árdua e, conforme a experiência internacional, morosa, sendo essa a maior problemática do mundo digital: a falta de padrões legais que ultrapassem as fronteiras nacionais em prol de um fluxo livre de dados. (REIDENBERG, 1998, p. 553-554, tradução nossa)[15]

Por fim, é importante ressaltar que decisões de adequação quando vinculadas à análise de um sistema legal podem ser demasiadamente demoradas. À título ilustrativo, Kuner (2009, p. 3) argumenta que existem 192 Estados-membros da Organização das Nações Unidas (ONU), ao subtrair os 36 Estados-membros da UE, da Associação Europeia de Comércio Livre (EFTA) e já considerados adequados perante o RGPD, restam 156 países passíveis de serem considerados adequados no âmbito europeu. Para efeitos de argumentação, pode-se então assumir que talvez metade destes países restantes nunca seriam considerados adequados por várias razões (e.g. falta de um sistema democrático de governo; um sistema jurídico funciona, dentre outros) restando assim 78 países possíveis candidatos à adequação.

---

[14] No original: "The purpose of adequacy decisions by the European Commission is to formally confirm, with binding effects on Member States including their competent data protection authorities, that the level of data protection in a third country or an international organisation is essentially equivalent to the level of data protection in the European Union. The third country should offer guarantees ensuring an adequate level of protection essentially equivalent to that ensured within the Union, in particular where data are processed in one or several specific sectors." (UNIÃO EUROPEIA, 2021, p. 6, tradução nossa)

[15] No original: "In the era of network and communications technologies, participants traveling on information infrastructures confront an unstable and uncertain environment of multiple governing laws, changing national rules, and conflicting regulations. For the information infrastructure, default ground rules are just as essential for participants in the Information Society as Lex Mercatoria was to merchants hundreds of years ago."

Em continuidade, pode-se assumir que as futuras decisões de adequação serão aprovadas ao mesmo ritmo que têm sido desde a entrada em vigor da Diretiva 95/16 (ou seja, a um ritmo de seis países aproximadamente em cada dez anos). Portanto, seriam necessários cerca de 130 anos para que os 78 países fossem considerados adequados ao RGPD.

Dessa forma, analisar caminhos alternativos que visem encurtar o período que pode ser demasiadamente longo é uma necessidade frente ao mundo globalizado. Portanto, acordos bilaterais podem ser um instrumento relevante de eficácia e rapidez frente as outras possibilidades existentes atualmente. Por isso, esta Monografia visa analisar este fenômeno alternativo que é a entabulação de um acordo bilateral.

1.3.2.2. Garantias suficientes

Na ausência de uma hipótese legal que autorize o livre fluxo dos dados entre o Brasil e outro país ou organismo internacional, a LGPD prevê uma segunda modalidade para permitir as transferências internacionais: as garantias suficientes. Similarmente às garantias adequadas previstas no Art. 46(2), do RGPD, a legislação brasileira permite a transferência internacional em seis hipóteses que proporcionem garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados da LGPD.

As hipóteses previstas levam em consideração que o controlador deve oferecer e comprovar que a LGPD está sendo cumprida, mesmo que o destinatário dos dados não seja um país considerado adequado à luz da LGPD. Para que a transferência internacional seja considerada legal, o controlador poderá adotar uma das seguintes medidas: (i) cláusulas contratuais específicas para determinada transferência; (ii) cláusulas-padrão contratuais; (iii) normas corporativas globais; (iv) selos; (v) certificados; e (vi) códigos de conduta. (BRASIL, 2018)

O controlador poderá se valer de cláusulas contratuais específicas para determinadas transferências internacionais, sendo que o agente de tratamento deverá submeter essas cláusulas à ANPD para verificação e aprovação, inclusive, em eventual alteração substancial de seu conteúdo. Sobre o seu conteúdo em específico, a LGPD preferiu não aprofundar o tema, sendo que o Art. 35, §1º, do referido diploma legal, prevê que deverão ser considerados os requisitos, as condições e as garantias

mínimas para a transferência que observem os direitos, as garantias e os princípios. (LEONARDI, 2021, p. 304)

Na mesma seara, as cláusulas-padrão contratuais são cláusulas-modelo elaboradas pela ANPD que, a depender de sua regulação, podem ser alteradas ou não. Ao adotar esse tipo de cláusula, o controlador poderá transferir os dados internacionalmente sem necessidade da intervenção da ANPD ou da anuência dos titulares dos dados. A cláusula-padrão contratual, na verdade, constitui um contrato que prevê direitos, obrigações e definições necessárias, de maneira similar aos *Data Processing Agreements* (Acordo de Tratamento de Dados – DPA). (LEONARDI, 2021, p. 304)

Novamente, na falta de regulação sobre o tema, importante analisar a experiência europeia que, geralmente, é acompanhada pela ANPD. A Comissão Europeia, desde a decisão de implementação nº 914/2021/EU[16], disponibiliza suas cláusulas-padrão contratuais (SCCs) em seu site[17], bem como orienta a maneira de sua utilização, sendo que o agente de tratamento poderá utilizar, para além das cláusulas gerais, módulos contratuais que se adaptem a sua realidade. (BERTOLDI, 2022, p. 1364, tradução nossa)[18]

Na mesma linha europeia, o *Information Commissioner's Office* (ICO) – que é a autoridade nacional de proteção de dados do Reino Unido – disponibiliza suas SCCs e orienta que sua adoção deve ser integral e sem alterações, sendo possível apenas a inclusão de cláusulas meramente comerciais e que não contrariem as SCCS, demonstrando, portanto, um modelo rígido de cláusulas-padrão contratuais. (LEONARDI, 2021, p. 304)

A timidez regulatória da ANPD sobre as transferências internacionais, em especial, a utilização de cláusulas-padrão contratuais coloca o Brasil alguns anos

---

[16] Decisão de implementação nº 914/2021/EU, datada de 4 de junho 2021, sobre cláusulas-padrão contratuais para a transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho. Disponível em: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. Acesso em: 17 jul. 2023.

[17] Comissão Europeia. **Standard Contractual Clauses for controllers and processors in the EU/EEA**. Disponível em: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en. Acesso em: 17 jul. 2023.

[18] No original: "One of the major innovations of Decision 914/2021/EU concerns the structure of the SCC. To adapt to different scenarios and to the growing complexity of modern processing data chains, general clauses are combined with a modular approach. In addition to general clauses, controllers and processors shall select the module that fits their situation, "so as to tailor their obligations under the standard contractual clauses to their role and responsibilities in relation to the data processing in question"."

longe de uma possível decisão de adequação pela UE. É impreciso afirmar a maneira como a ANPD interpretará estes mecanismos, entretanto, pode-se vislumbrar uma possível regulação que vá ao encontro das práticas europeias sobre o tema.

Outro mecanismo de garantias de cumprimento da LGPD é a norma corporativa global. O referido instrumento pode ser utilizado para transferência internacional entre empresas do mesmo grupo econômico, semelhante às BCRs do RGPD. Embora a LGPD seja omissa a respeito, vislumbra-se que a ANPD adote o mesmo modelo europeu com um conteúdo mínimo e sua aprovação prévia pela autoridade competente. Nesses termos, importa citar Leonardi (2021, p. 305):

> Em geral, as BCRs devem conter os princípios de proteção de dados pessoais, como transparência, qualidade e segurança, os meios que garantem a efetividade da política interna do grupo (auditoria, treinamento etc.) e mecanismos que comprovem que a política seja, de fato, vinculante para as empresas do grupo. É importante compreender que o conteúdo das BCRs não é limitado a transferências internacionais, descrevendo quais são os principais procedimentos internos, políticas e outras medidas administrativas, organizacionais e técnicas adotadas por todo o grupo para a proteção de dados pessoais. Caso o grupo tenha suas BCRs aprovadas, todas as transferências internacionais de dados pessoais intragrupo passam a estar em conformidade com o GDPR, não sendo necessário obter nova autorização da autoridade para realizá-las.

E, por fim, as três últimas ferramentas são selos, certificados e códigos de conduta devidamente aprovados pela ANPD ou por um organismo de certificação designado por ela e devidamente credenciado, conforme o Art. 35, §3º, da LGPD. De igual forma as outras ferramentas descritas anteriormente, não há qualquer regulamentação que aponte uma direção correta para quais selos, certificados e códigos de conduta são válidos ou até qual o procedimento de avaliação destes documentos, na verdade, o que se tem são apenas os requisitos genéricos mínimos estampados no Art. 35, §1º, da LGPD. (LEONARDI, 2021, p. 305)

Igualmente às ferramentas abordadas anteriormente, a comunidade europeia avançou nestes quesitos, tendo o EDPB publicado diretrizes e recomendações que delimitaram a utilização de certificados, códigos de conduta e normas corporativas globais como ferramentas que viabilizam transferências internacionais no velho continente.[19]

[19] As diretrizes e recomendações publicadas pelo EDPB são diversas: Diretriz nº 04/2021 sobre Códigos de Conduta como ferramentas para transferências; Diretriz nº 07/2022 sobre certificação como ferramenta para transferência; e a Recomendação nº 1/2022 sobre o pedido de homologação e sobre os elementos e princípios que constam das Normas Corporativas Globais do controlador. Disponível

1.3.2.3. Exceções legais

Para além dos mecanismos previstos anteriormente (i.e., decisão de adequação e utilização de ferramentas que garantam o cumprimento da LGPD), a legislação de proteção de dados brasileira previu outras hipóteses que se tratam verdadeiras exceções legais correlatas às derrogações do Art. 49, do RGPD (VERONESE, 2021, p. 717). As exceções legais estão listadas nos incisos III ao IX, do Art. 33, da LGPD, que totalizam nove hipóteses:

> III – quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> IV – quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> V – quando a autoridade nacional autorizar a transferência;
> VI – quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> VII – quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
> VIII – quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou IX – quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7.º desta Lei. (BRASIL, 2018)

Ademais, o último inciso do Art. 33, da LGPD, prevê outras três hipóteses que são derivadas do Art. 7º, da LGPD, sendo elas: (i) para cumprimento de obrigação legal ou regulatória pelo controlador; (ii) quando necessário para a execução de contrato ou procedimento preliminares relacionados a contrato, a pedido do titular dos dados; e (iii) para o exercício regular de direitos em processos judiciais, administrativos e/ou arbitrais. (BRASIL, 2018).

Na primeira hipótese, tem-se a autorização da transferência quando necessária à cooperação jurídica internacional entre órgãos de inteligência e investigação, sendo, nas palavras de Leonardi (2021, p. 305), uma “hipótese restrita, em que o interesse público se sobrepõe aos direitos dos titulares dos dados pessoais transferidos, sem aplicação direta para o setor privado.”. À título exemplificativo, esta exceção legal pode auxiliar os procedimentos de requisição via Acordo de Assistência

---

em: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en?f%5B0%5D=opinions_topics%3A747&page=0. Acesso em: 18 jul. 2023.

Judiciária em Matéria Penal (*Mutual Legal Assistance in Criminal Matters* – MLAT), instrumento que visa requisitar dados diretamente de servidores de internet sediados no exterior.

Ademais, há outras três hipóteses que estão contidas também nas bases legais que autorizam o tratamento de dados pessoais. A transferência internacional é autorizada para fins de proteção da vida, sendo um caminho constante delineado pelo legislador há anos na proteção do maior bem jurídico que é a vida. Para fins de execução de política pública, apenas pela Administração Pública, sendo necessário garantir a devida publicidade e transparência – princípios norteadores da Administração Pública – da transferência internacional, nos termos do Art. 23, da LGPD. Por último, o controlador de dados poderá transferir internacionalmente com base no consentimento do titular dos dados.

O consentimento enquanto hipótese legal que permite transferência internacional de dados não se distingue daquele utilizado como base legal para tratamento de dados pessoais. Quando a transferência for realizada utilizando o consentimento, este deverá o ser obtido especificamente para tal fim, recebendo o devido destaque e informado previamente ao titular dos dados. Além de seguir com os requisitos para transferência internacional, o consentimento deverá ser baseado em todas as outras disposições da LGPD, sendo livre, informado e inequívoco para finalidades definidas, podendo ser revogado a qualquer tempo.

Diante das inúmeras peculiaridades e requisitos que o consentimento possui até como base legal para o tratamento de dados pessoais, a sua utilização para transferências internacionais acaba se dando apenas teoricamente. Na prática, a sua aplicação é demasiadamente complexa e se mostra inviável em larga escala para o setor privado. (LEONARDI, 2021, p. 307)

Além das exceções legais dispostas anteriormente, a LGPD prevê que as bases legais que autorizam o tratamento de dados pessoais no Art. 7º sejam utilizadas para transferir dados internacionalmente. Para a obrigação legal ou regulatória, a transferência internacional delimita a sua finalidade específica, sendo que não há qualquer interpretação da ANPD sobre a necessidade iminente nacional da obrigação legal.

No mesmo sentido, a transferência internacional poderá ser realizada quando necessária para execução de contrato ou procedimento pré-contratual, sendo indispensável que o titular dos dados seja parte. (LEONARDI, 2021, p. 307).

Importante ressaltar, o RGPD prevê a existência da mesma exceção legal, todavia, impôs limitações em seu uso apenas para execução de contrato de forma eventual, conteúdo não replicado pela LGPD. (CONSELHO DA EUROPA; PARLAMENTO EUROPEU, 2016, tradução nossa)[20]

A outra exceção legal se relaciona com o exercício regular de direitos em processos judiciais, administrativos ou arbitrais. De forma coerente com o texto constitucional, o legislador incluiu essa hipótese a fim de garantir os princípios do contraditório e ampla defesa, ressalta-se, tanto ao controlador como aos titulares dos dados e/ou terceiros.

As últimas duas hipóteses de exceção legal não contêm disposições claras acerca de sua aplicação. Com base na autorização da ANPD, o controlador dos dados poderia transferi-los internacionalmente, no entanto, mais um assunto que deverá aguardar seu esclarecimento pela ANPD. Do outro lado, há a hipótese de transferência com base em acordo de cooperação internacional, sem muitos detalhes e deveras genérico conta ainda com um erro material: “se lê “resultar em”, leia-se “resultar de” – obviamente, a transferência é o resultado do compromisso assumido, e não o fato gerador desse compromisso.”. (LEONARDI, 2021. p. 306).

Isto posto, a LGPD acompanha o RGPD na maior parte de seus dispositivos que tratam sobre transferência internacional de dados pessoais. Nas palavras de Veronese (2021, p. 719):

> Assim, ressalvada a opção prevista no inciso V do art. 33 da LGPD, todas as demais hipóteses são similares com exceções previstas no RGPD: os incisos III e VI fazem parelha com o artigo 48.º do RGPD; o inciso IV corresponde à alínea “f ” do parágrafo 1.º do n. 1 do artigo 49.º do RGPD; o inciso VII tem similitude com as alíneas “d” e “g” do mesmo dispositivo do RGPD; o inciso VIII está alinhado com a alínea “a” dele; o inciso IX, combinado com os incisos II e VI do art. 7.º da LGPD, são similares à alínea “e” do parágrafo 1.º do n. 1 do artigo 49.º do RGPD, apesar de terem uma maior abrangência, pois incluem processos administrativos e arbitrais, além de indicarem o suprimento de obrigações legais e regulatórias; e, por fim, o inciso IX, combinado com o inciso V do artigo 7.º da LGPD, amoldam-se às alíneas “b” e “c” do parágrafo 1.º do n. 1 do artigo 49.º do RGPD, apesar de não indicarem a execução de um contrato, diferentemente do que está no RGPD. Do simples cotejo entre a LGPD e o RGPD é possível identificar, de forma geral, que a legislação brasileira tem a norma jurídica europeia como modelo.

[20] Com base no Considerando (111) do RGPD. No original: “Provisions should be made for the possibility for transfers in certain circumstances where the data subject has given his or her explicit consent, where the transfer is occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies.”

Conclui-se, portanto, esta primeira Seção que se propôs evidenciar os mecanismos existentes na LGPD e sua correlação com a RGPD. Entender essa correspondência entre ambas as legislações de proteção de dados é necessária para delinear uma análise crítica relacionada a entabulação de acordos bilaterais entre UE e EUA como mecanismos de transferência internacional. A próxima Seção se baseará nos acordos bilaterais firmados e os motivos que levaram a sua derrocada.

2. ACORDOS BILATERAIS DE TRANSFERÊNCIA INTERNACIONAL DE DADOS

Esta Seção será responsável por abordar os acordos firmados entre o velho continente e os estadunidenses para fins de legalizar as transferências internacionais de dados. Para a persecução da análise destes acordos, o objeto de estudo está delimitado nos seguintes acordos bilaterais: *Safe Harbor Agreement*, *Privacy Shield* e *Data Privacy Frameworks*. No mais, a análise dos acordos também considerará as decisões emanadas pela Corte de Justiça da União Europeia (CJUE) na invalidação dos dois primeiros acordos mencionados anteriormente.

2.1. *SAFE HARBOR AGREEMENT* (ACORDO DO PORTO SEGURO)

A crescente globalização e intensificação do comércio entre o bloco europeu e os EUA proporcionou um terreno fértil para considerações acerca do compartilhamento de informações. A origem do *Safe Harbor* está vinculada à necessidade econômica dos EUA receber, legalmente, dados pessoais de cidadãos europeus, que, no início do novo século, estavam em um momento de desenvolvimento propício para a criação em massa de dados.

2.1.1. Conteúdo legal para transferência internacional de dados

Com negociações iniciadas ainda em 1998 entre o Departamento de Comércio dos EUA e a Comissão Europeia (SCHARTZ, 2013, p. 1980), a necessidade de se criar um padrão legal de transferência de dados cresceu pelo tamanho do mercado – leia-se o número de habitantes na UE que produzem inquantificáveis número de dados pessoais – proporcionado aos EUA. O tema se acentuou em vista da concentração de empresas de tecnologia nos EUA, criando, assim, a grande dicotomia entre as partes: de um lado, os EUA precisavam legalizar e expandir o tratamento de dados de cidadãos europeus; e por outro lado, a UE precisava avançar com sua proteção de dados para além das fronteiras de seus membros. (SCHWARTZ; PEIFER, 2017, p. 158)

Assim, sob o comando da Diretiva 95/46/CE, foi-se entabulado o primeiro acordo de transferência internacional de dados: o *Safe Harbor (*em tradução livre:

Porto Seguro). Os Arts. 25 e 26 da referida Diretiva estabeleciam o regime jurídico que regeria o intercâmbio de dados pessoais para países fora do espaço econômico europeu, sendo que a análise ficaria à conta da garantia de um nível de proteção adequado em razão de sua legislação interna ou compromisso internacional. (NI LOIDEAN, 2016, p. 8)

A partir do comprometimento internacional dos EUA, em 26 de julho de 2000, a Comissão Europeia publicou a Decisão 2000/520/EC entendendo que o *Safe Harbor* (Anexo I da decisão) e o FAQ (uma espécie de questões frequentes relacionadas ao acordo) “asseguram um nível adequado de proteção dos dados pessoais transferidos a partir da Comunidade Europeia para organizações estabelecidas nos Estados Unidos da América”. (UNIÃO EUROPEIA, 2000, p. 4)

O *Safe Harbor Agreement* buscou harmonizar duas abordagens regulatórias de proteção de dados e privacidade distintas (NI LOIDEAN, 2016, p. 8). Por meio de um programa voluntário de auto certificação em relação aos princípios contidos no Safe Harbor (SANTOS; VERONESE, 2021, p. 118), as transferências internacionais de dados foram regulamentadas e exigiu que empresas estadunidenses fossem submetidas aos padrões de proteção de dados mais elevados. (SANTOS; VERONESE, 2021, p. 118 *apud* BERMAN, 2006, p. 1127)

O referido acordo de transferência internacional de dados estabeleceu sete princípios de privacidade constantes em seu Anexo I. Notadamente, os princípios de porto seguro são: aviso, escolha, transferência posterior, segurança, integridade dos dados, acesso e aplicação. Necessário, portanto, delinear brevemente as disposições dos princípios contidos no Safe Harbor.

O princípio do aviso, muito próximo do que se tem no ordenamento jurídico brasileiro em relação ao princípio da finalidade e transparência, determinava que as empresas deveriam informar aos titulares de dados a finalidade do tratamento, a forma de contato para exercício de seus direitos, o compartilhamento de dados com terceiros e maneiras para limitar o tratamento destes dados. Adicionalmente, previu-se a necessidade de que as informações fossem prestadas de maneira clara e visível aos titulares de dados, bem como na primeira oportunidade que se referia o tratamento de dados pessoais. (UNIÃO EUROPEIA, 2000, p. 8)

No que tange ao princípio da escolha, o *Safe Harbor* previa mecanismos que garantia a faculdade do titular de dados escolher (por meio de *opt in* ou *opt out*) sobre o compartilhamento de dados com terceiros e o tratamento dos dados para finalidade

diversa daquele inicialmente prevista no momento da coleta. Quando se tratasse de dados pessoais sensíveis, o acordo previa uma escolha afirmativa e explicita do titular de dados pessoais para o tratamento. (UNIÃO EUROPEIA, 2000, p. 8)

Após o cumprimento dos princípios do aviso e da escolha, por meio do princípio da transferência posterior se criou a obrigatoriedade do agente de tratamento, ao transferir dados para terceiros, garantir que estes terceiros cumpram os princípios do Porto Seguro, as disposições da Diretiva 95/46/CE ou outras disposições adequadas. Importante ressaltar, o agente de tratamento originário estaria eximido de responsabilidade dos terceiros, caso cumprisse com os requisitos mencionados anteriormente. (UNIÃO EUROPEIA, 2000, p. 9)

O princípio da segurança determinava que as empresas deveriam tomar medidas razoáveis para evitar a perda, utilização indevida e acesso, revelação, alteração ou destruição não autorizados. (UNIÃO EUROPEIA, 2000, p. 9) Também conhecido no ordenamento jurídico brasileiro, este princípio garante que os titulares de dados tenham a expectativa da segurança de seus dados, a partir de medidas técnicas e operacionais que as garantisse.

A integridade dos dados pessoais também estava prevista como um princípio que deveria balizar as transferências internacionais. Assim, vedava-se o tratamento incompatível com a finalidade para os quais os dados foram coletados, dialogando, portanto, com o princípio da escolha. Além disso, garantia-se que os dados pessoais fossem precisos, atualizados e completos. (UNIÃO EUROPEIA, 2000, p. 9)

A partir do princípio do acesso, os titulares de dados tinham o direito de acessar os dados pessoais transferidos, bem como a potestatividade de retificá-los, alterá-los ou eliminá-los. A própria disposição deste princípio criou uma exceção, as empresas poderiam recusar o acesso caso a despesa de fornecê-lo seja desproporcional aos riscos para a privacidade do titular ou quando os direitos de outros titulares possam ser violados por este acesso. (UNIÃO EUROPEIA, 2000, p. 9)

Por fim, mas não menos importante, previu-se o princípio da aplicação (em inglês, *enforcement*), sendo garantido aos titulares de dados mecanismos que cumpram com os princípios de porto seguro, recursos independentes e sanções em caso de violação. Portanto, criou-se um modelo de execução do *Safe Harbor* baseado em obrigações de garantia da contestação das transferências internacionais pelos titulares de dados, privilegiando, assim, uma autodeterminação informativa. (UNIÃO EUROPEIA, 2000, p. 9).

Como será exposto a seguir, o *Safe Harbor* não foi capaz de garantir a proteção de dados pessoais dos titulares europeus, especificamente no que se tange ao acesso, pelas autoridades públicas estadunidenses, aos dados pessoais. Nestes termos, ensina Santos e Veronese (2021, p. 119):

> A despeito do otimismo à época da conclusão do acordo, com o tempo, críticas relativas ao Safe Harbor foram se intensificando e cada vez mais entidades passaram a acompanhá-las. O próprio Grupo de Trabalho "Artigo 29" que, em 2000, havia divulgado parecer favorável, sustentando ser o Safe Harbor "um marco de progresso para o aprimoramento da proteção de dados", passou a compreendê-lo como "questionável". Em especial, as revelações de Edward Snowden impactaram negativamente a confiança nos fluxos de dados pessoais por sobre fronteiras entre a UE e os EUA. O Safe Harbor Agreement estava no centro das preocupações, tendo a próprio Comissão Europeia questionado a eficácia de sua proteção e emitido recomendações para a melhoria do acordo.

2.1.2. Decisão TJUE no processo C-362/14 (Schrems I)

Após a entabulação do Safe Harbor em 2000, a comunidade europeia precisou lidar com um grande escândalo envolvendo a privacidade de seus dados devido à exceção contida no preâmbulo do acordo, veja-se: "A adesão a estes princípios pode ser limitada: a) na medida necessária para observar requisitos de segurança nacional, interesse público ou execução legal [...]". (UNIÃO EUROPEIA, 2000, p. 7).

O escândalo envolvendo Edward Snowden e a *National Security Agency* (NSA) revelou uma reação justificada do austríaco Maximillian Schrems em 25 de junho de 2013. (SANTOS; VERONESE, 2021, p. 119-120) A sua principal consideração era em relação à utilização pelo governo estadunidense do sistema PRISM que inicialmente foi criado para rastrear estrangeiros suspeitos de terrorismo, mas que na vil verdade realizada uma coleta em massa de dados sem qualquer distinção de usuários. (ESTADÃO, [2013]) Portanto, Schrems alegou que não havia qualquer proteção significativa na lei ou na prática dos EUA em relação à privacidade, principalmente em relação à exceção de segurança nacional. (NI LODEAN, 2016, p. 9)

No âmbito regional de proteção de dados, o estudante de direito austríaco apresentou uma denúncia à Autoridade de Proteção de Dados Irlandesa (APD) alegando que a transferência internacional de dados de cidadãos europeus para os

EUA[21] era incompatível com as regras de privacidade estabelecidas na UE e, portanto, seus dados deveriam ser proibidos de serem transferidos. (NI LOIDEAN, 2016, p. 9)

A APD, por sua vez, declinou sua competência, considerando que a Comissão Europeia já havia proferido decisão considerando adequado o instrumento de transferência internacional de dados: o *Safe Harbor*. Schrems recorreu à Suprema Corte irlandesa que encaminhou seus questionamentos ao TJUE. (SANTOS; VERONESE, 2021, p. 120) A partir deste momento, o acordo bilateral foi questionado e, em 6 de outubro de 2015, invalidado pela TJUE.

O TJUE considerou que a exceção contida em relação à segurança nacional deveria operar na estrita medida do necessário, uma vez que tinha a capacidade de cercear direitos fundamentais de cidadãos europeus. Nestes termos, o TJUE (2015, p. 25) se manifestou:

> Assim, não é limitada ao estritamente necessário uma regulamentação que autoriza de modo generalizado a conservação da totalidade dos dados pessoais de todas as pessoas cujos dados foram transferidos da União para os Estados Unidos sem qualquer diferenciação, limitação ou exceção em função do objetivo prosseguido e sem que esteja previsto um critério objetivo que permita delimitar o acesso das autoridades públicas aos dados e a sua utilização posterior para fins precisos, estritamente limitados e suscetíveis de justificar a ingerência que tanto o acesso como a utilização desses dados comportam [...]

Adicionalmente, o TJUE considerou que o Safe Harbor inviabilizou o direito de o titular de dados recorrer às vias de direito para ter acesso, retificar ou excluir seus dados e, portanto, isto violaria o direito fundamental a uma proteção jurisdicional efetiva. (UNIÃO EUROPEIA, 2015, p. 25) Assim, concluiu que as transferências internacionais só poderiam ser válidas caso o agente importador de dados oferecesse um nível adequado[22] de proteção que, obviamente, não deveria ser idêntico, mas

---

[21] Neste ponto, faz-se necessário entender a dinâmica da transferência internacional questionada. Conforme se depreende do Acórdão de 6 de out. de 2015 do TJUE, todo cidadão europeu que utilizasse a rede social Facebook "são obrigadas, no momento da sua inscrição, a celebrar um contrato com a Facebook Ireland, filial da Facebook Inc., com sede nos Estados Unidos. Os dados pessoais dos utilizadores do Facebook residentes no território da União são, no todo ou em parte, transferidos para servidores pertencentes à Facebook Inc., situados em território dos Estados Unidos, onde são objeto de tratamento." (UNIÃO EUROPEIA, 2015, p. 15)

[22] Nos termos do acórdão emanado pelo TJUE (2015, p. 22): "deve ser entendida no sentido de que exige que esse país terceiro assegure efetivamente, em virtude da sua legislação interna ou dos seus compromissos internacionais, um nível de proteção das liberdades e direitos fundamentais substancialmente equivalente ao conferido dentro da União nos termos da Diretiva 95/46, lida à luz da Carta."

deveria levar ao mesmo resultado que a proteção europeia. (SANTOS; VERONESE, 2021, p. 120)

As práticas perpetradas pelo governo estadunidense para suposta garantia da segurança nacional levaram à derrocada do *Safe Harbor*, tendo a TJUE enfatizado a necessidade de um nível adequado de privacidade que proteja seus cidadãos. (NI LOIDEAN, 2016, p. 11) A partir deste ponto, um novo acordo bilateral precisou ser delineado e, assim, nasceu o *Privacy Shield*.

2.2. *PRIVACY SHIELD* (ESCUDO DE PRIVACIDADE)

O mundo que foi transformado pela globalização e pela criação da internet entendeu a necessidade das transferências internacionais de dados para o desenvolvimento econômico, avanço tecnológico e interação social. (KUNER, 2017, p. 882) Portanto, a partir de Schrems I, a UE e os EUA ainda necessitavam de uma ferramenta bilateral que regulasse estas transferências, assim, criou-se o *Privacy Shield*.

2.2.1. Conteúdo legal para transferência internacional de dados

Em 2 de fevereiro de 2016, aproximadamente quatro meses após a invalidação do *Safe Harbor*, os EUA e a UE chegaram a um novo acordo que viabilizaria as transferências internacionais. Assim, em 12 de julho de 2016, a Comissão Europeia publicou sua decisão de adequação do *Privacy Shield*, considerando que o novo mecanismo era essencialmente equivalente às leis da UE, após algumas alterações, inclusive, na legislação interna estadunidense. (KUNER, 2017, p. 883)

Apesar da entabulação de um novo acordo bilateral, o *Privacy Shield* era similar ao *Safe Harbor*, prevendo princípios e princípios suplementares mais detalhados, onde as empresas se auto certificariam sua conformidade. Entretanto, conforme menciona Kuner (2017, p. 903, tradução nossa), em contraste ao *Safe Harbor*, o *Privacy Shield* inclui “compromissos de autoridades de segurança nacional

dos EUA relativamente às proteções concedidas aos dados de cidadãos da UE, bem como cartas e declarações de outros funcionários do governo dos EUA".[23]

Com a proposta de um *Safe Harbor* 2.0., o *Privacy Shield*, em tese, havia aprimorado seu *framework* legal, a fim de garantir efetividade aos direitos dos titulares europeus. Como ressaltado por Santos e Veronese (2021, p. 122), o novo acordo previu obrigações robustas para as empresas estadunidenses, um monitoramento pelo Departamento de Comércio com a possibilidade de aplicação de sanções a quem descumprisse-o, um aumento nas limitações dos órgãos de inteligência estadunidenses contando com revisões anuais pela UE e a possibilidade de reparação dos titulares de dados estadunidenses.

Ainda sob o ordenamento da Diretiva 95/46/CE, mas já contando com a aprovação do RGPD, o *Privacy Shield* continuou enfrentando inúmeros problemas relacionados a sua estabilidade. Santos e Veronese (2021, p. 123) mencionam que "a afirmação do Presidente dos EUA, Donald Trump, de que iria revogar todas as ordens executivas emitidas pelo ex-Presidente Barack Obama" causaram um problema inicial, uma vez que os compromissos de privacidade assumidos pelo EUA estavam essencialmente constituídos nestas ordens executivas.

Em virtude de o novo acordo ter sido entabulado anteriormente à vigência do RGPD, o *Privacy Shield* não considerou as novas regras adicionadas ao *framework* de proteção de dados europeu. Por este motivo, a Decisão nº 2016/1250 da Comissão Europeia que considerou o acordo adequado previu a possibilidade de suspensão do acordo após a data de aplicação do RGPD (UNIÃO EUROPEIA, 2016, p. 34)[24], a fim de avaliar novamente o nível de proteção do *Privacy Shield*. (KUNER, 2017, p. 903-904)

Ao conter versões mais fracas de alguns princípios de privacidade da UE (SCHWARTZ; PEIFER, 2017, p. 47), o *Privacy Shield* concentrou sua matriz legal em quatro princípios fundamentais: integridade dos dados e limitação da finalidade, escolha, aplicação e supervisão. Estes princípios criaram o core do acordo e tentaram,

[23] No original: "In contrast with the Safe Harbour, the Privacy Shield also includes commitments from US national security officials concerning protections given to data from EU citizens, as well as letters and statements from other US government officials."

[24] Neste sentido, uma nota de rodapé prevista no item de suspensão da decisão de adequação continha o seguinte teor: "A partir da data de aplicação do Regulamento Geral sobre a Proteção de Dados, a Comissão utilizará os seus poderes para adotar, por imperativos de urgência devidamente justificados, um ato de execução de suspensão da presente decisão, que será aplicável imedia- tamente sem a sua apresentação prévia ao respetivo comité de comitologia e permanecerá em vigor durante um período máximo de seis meses."

na medida do possível, trazer novas salvaguardas a partir da experiência do Schrems I.

O princípio diz respeito à integridade dos dados e limitação da finalidade de tratamento, algo presente no *Safe Harbor* (i.e., princípio da integridade de dados), mas neste caso com uma linguagem específica que enfatiza a existência de uma proibição expressa do tratamento posterior incompatível com àquele informado ao titular de dados. (SCHWARTZ; PEIFER, 2017, p. 161)[25] Ademais, o acordo criou um requisito para a limitação da finalidade - as transferências ulteriores – fazendo com que as empresas precisem garantir que as transferências com terceiros sejam no limite da finalidade para a qual os dados foram coletados. Por meio do uso de contratos "*business-to-business*", as empresas deveriam garantir que este contrato forneça o mesmo nível de proteção do *Privacy Shield*, também utilizando SCCs. (SCHWARTZ; PEIFER, 2017, p. 162)

O próximo princípio abordado é o da escolha, este que estabelece o direito de *opt in* e *opt out* para os titulares de dados europeus. Ainda neste tema, o *Privacy Shield* previu que o consentimento expresso e afirmativo do titular é necessário no caso de tratamento de dados sensíveis, sendo necessário um controle rígido do consentimento nas transferências internacionais. (SCHWARTZ; PEIFER, 2017, p. 163)

No caso do *opt out*, o *Privacy Shield* inova em relação ao *Safe Harbor* ao criar uma exceção para as operações de tratamento de dados que sejam materialmente alteradas, mas ainda compatíveis com a finalidade originária. Neste sentido, ensina Schwartz e Peifer (2017, p. 163):

> Cria uma nova categoria dentro da compatibilidade que, de outra forma, seria desconhecida na legislação de proteção de dados da UE. Prevê uma operação de processamento "materialmente alterada, mas ainda compatível", que está sujeita a uma opção de exclusão. Esta linguagem representa uma concessão da UE aos Estados Unidos; aceita a possibilidade de que uma mudança "material" na finalidade possa, no entanto, ainda estar suficientemente próxima da finalidade original da recolha para não exigir outra ronda de consentimento individual. [...][26]

[25] Neste sentido, a Decisão nº 2016/1250 (2016, p. 4) prevê: "No âmbito do princípio de integridade dos dados e limitação dos fins, os dados pessoais devem limitar-se ao que é relevante para o fim do tratamento, ser fiáveis para a utilização prevista, exatos, completos e atuais. Uma organização não pode tratar dados pessoais de modo incompatível com o fim que motivou a recolha original ou que tenha sido autorizado posteriormente pelo titular dos dados. As organizações devem assegurar que os dados pessoais são fiáveis em relação à utilização prevista, exatos, completos e atuais."

[26] No original: "It creates a new category within compatibility that is other- wise unknown to EU data protection law. It envisions a "materially changed, but still compatible" processing operation, which is made subject to an opt- out.298 This language represents an EU concession to the United States; it

Em relação ao princípio da aplicação, mais robusto do que previsto no Safe Harbor, criou-se mecanismos gerais de aplicação e um subconjunto de ferramentas no caso de agências de inteligência dos EUA. O *Privacy Shield* previu a possibilidade de o titular dos dados apresentar reclamação a uma empresa certificada, acionar a sua autoridade regional em caso de violações, utilizar o sistema de resolução alternativa de litígios a partir do *Privacy Shield Panel*, uma espécie de mecanismo de arbitragem que cria decisões vinculativas às empresas estadunidenses. (SCHWARTZ; PEIFER, 2017, p. 164)

Por fim, o *Privacy Shield* criou o princípio da supervisão, aquele responsável, por meio de um procedimento específico, avaliar a aderência efetiva das empresas aos mecanismos de transferência internacional, não só, mas também de monitorar como as agências de inteligência estadunidense atuam na proteção de dados dos cidadãos europeus. Neste sentido, ensina Santos e Veronese (2021, p. 122) "Do ponto de vista de um titular de dados pessoais, na UE, o *Privacy Shield* ofereceria melhorias em comparação ao instrumento invalidado pelo TJUE, sobretudo quanto aos aspectos práticos de supervisão e de reparação, além de dispositivos mais detalhados.".

Como se verá a seguir, o *Privacy Shield* foi novamente questionado a partir do caso Schrems II e, consequentemente, invalidado pela TJUE. Após a decisão de invalidação do Safe Harbor, o caso retornou à APD irlandesa que havia declinado a competência, entretanto, na investigação reinstaurada o Facebook Irlanda alegou que seus dados agora eram transferências com base nas SCCs. Este ponto foi de alta relevância, uma vez que as bases jurídicas de contestação das transferências internacionais eram distintas (ora se falava de Safe Harbor, ora de SCCs), mas tinham algo em comum: o padrão de proteção oferecido pelos EUA. (SANTOS; VERONESE, 2021, p. 123)

2.2.2. Decisão TJUE no processo C-311/18 (Schrems II)

Após a alegação do Facebook Irlanda, a APD instou Schrems a reformular sua reclamação sobre as transferências internacionais, este, por sua vez, realizou uma nova reclamação em 1 de dezembro de 2015 requerendo a invalidação das SCCs

---

accepts the possibility that a "material" change in purpose may nonetheless still be close enough to the *original purpose of collection not to require another round of individual consent*."

utilizadas pela empresa, sob os mesmos argumentos anteriores. A APD encaminhou a matéria à Corte Superior europeia que, por conseguinte, encaminhou as questões ao TJUE, incluindo, o nível de proteção dos dados pessoais fornecido pelo *Privacy Shield*. (SANTOS; VERONESE, 2021, p. 124)

Posteriormente, em 16 de julho de 2020, o TJUE proferiu seu acórdão que declarou o *Privacy Shield* inválido. (UNIÃO EUROPEIA, 2020, p. 50). Isto pois, o acesso por sistemas de vigilância (neste caso se falava nos sistemas baseados na Seção 702 da FISA) no território estadunidense é frontalmente contrário às "exigências que garantam, no cumprimento do princípio da proporcionalidade, um nível de proteção substancialmente equivalente". (UNIÃO EUROPEIA, 2020, p. 45)

Dessa forma, o TJUE entendeu que os sistemas de inteligência estadunidense não garantem limitações à coleta massiva de dados pessoais, sequer produzem garantias para as pessoas "não americanas potencialmente visadas por esses programas" (UNIÃO EUROPEIA, 2020, p. 46) Ademais, o TJUE asseverou que o próprio governo dos EUA informou que não conferem aos titulares de dados direitos oponíveis às autoridades estadunidenses nos tribunais.

A problemática girou em torno da falta da possibilidade de oposição ao tratamento de dados de cidadãos europeus por agências de inteligência estadunidenses, neste sentido, contrariando o artigo 45 (2), a, do RGPD, que agora se aplicaria ao acordo firmado. Portanto, o TJUE (2020, p. 47) se manifestou da seguinte forma:

> Nestas condições, as limitações da proteção de dados pessoais que decorrem da regulamentação interna dos Estados Unidos relativa ao acesso e à utilização, pelas autoridades públicas americanas, desses dados transferidos da União para os Estados Unidos, e que a Comissão avaliou na Decisão BPD, não estão enquadradas de forma a satisfazer os requisitos substancialmente equivalentes aos exigidos, no direito da União, no artigo 52º, nº 1, segundo período, da Carta.

Indo além dos argumentos essencialmente envolvendo o RGPD e o *Privacy Shield*, o TJUE ainda trouxe à tona a violação ao direito fundamental à proteção jurisdicional efetiva, uma vez que a inexistência de mecanismos que garantam o exercício dos direitos dos titulares de dados (e.g. acesso, retificação, exclusão) contrariam o próprio Estado Democrático de Direito. (UNIÃO EUROPEIA, 2020, p. 47)

Apesar de originalmente prever mecanismos de resolução de conflitos, o *Privacy Shield* era ineficaz, uma vez que as decisões tomadas nestes mecanismos de

resolução não cabiam via recursal. (UNIÃO EUROPEIA, 2020, p. 48) Portanto, a Decisão nº 2016/1250 da Comissão Europeia que considerou o acordo adequado foi considerada inválida, uma vez que, na prática, o *Privacy Shield* não proporcionava um nível de proteção essencialmente compatível com o RGPD.

No que tange às SCCs utilizadas pelo Facebook Irlanda para transferências internacionais, o TJUE entendeu que estas continuariam válidas e pontuou que deveria haver uma análise "para o agente que exportar e para aquele que importa os dados pessoais de verificar, antes da transferência, se o nível de proteção é respeitado no destino, assim como comunicar qualquer impossibilidade de cumprimento das cláusulas" (SANTOS; VERONESE, 2021, p. 126). Nestes termos, delineou-se, novamente, a necessidade da entabulação de um novo acordo bilateral entre os EUA e a UE, o que aconteceria alguns anos depois.

2.3. *DATA PRIVACY FRAMEWORK* (MARCO LEGAL DA PRIVACIDADE)

Após o decurso de três anos, em julho de 2023, a Comissão Europeia, após inúmeras negociações com o governo estadunidense, publicou a Decisão nº 2023/1795 de adequação do novo acordo bilateral: o *Data Privacy Framework*[27]. Esforços dos estadunidenses foram levados em consideração, isto pois, em 7 de outubro de 2022, o presidente americano havia publicado uma ordem executiva com novas limitações nas atividades de coleta de dados pessoais em atividades de inteligência. (ESTADOS UNIDOS DA AMÉRICA, 2023)

Como os outros acordos firmados anteriormente, o *Data Privacy* nasceu do confronto com Philippe Latombe, um membro do parlamento francês e comissário da Autoridade de Proteção de Dados francesa (CNIL). Numa entrevista, Latombe (2023, tradução nossa) disse:

> O texto resultante destas negociações viola a Carta dos Direitos Fundamentais da União, devido às garantias insuficientes de respeito pela vida privada e familiar no que diz respeito à recolha em massa de dados pessoais, e o Regulamento Geral de Proteção de Dados (RGPD), devido à ausência de garantias de direito a um recurso efetivo e acesso a um tribunal imparcial, à ausência de um quadro para decisões automatizadas ou à falta de garantias relativas à segurança dos dados tratados: todas as violações da

[27] Um site foi criado pelo governo estadunidense para as empresas se auto certificarem e entenderem o teor do Data Privacy Framework. Disponível em: https://www.dataprivacyframework.gov/s/. Acesso em: 4 out. 2023.

> nossa lei que desenvolvo em o escrito de 33 páginas (+ 283 páginas de anexos) protocolado ontem no TJUE.[28]

Mesmo diante das críticas, o *Data Privacy* incluiu ajustes necessários a partir dos casos Schrems I e II, como, por exemplo, instrumentos de reparação às transferências internacionais com a criação de um Tribunal de Revisão da Proteção de Dados (*Data Protection Review Court*) que terá competência para analisar qualquer fluxo transatlântico de dados, independente do instrumento utilizado. (BRYANT, 2023) Além disso, as vias administrativas e judiciais recursais foram previstas para que o titular de dados possa exercer seus direitos plenamente. (UNIÃO EUROPEIA, 2023, p. 131)

Ademais, foi-se incentivada a Avaliação de Impacto das Transferências (TIA), documento este, elaborado pelo agente de tratamento responsável, que poderá demonstrar previamente se aquela transferência internacional poderá impactar os direitos dos titulares. Neste caso, aplicável tanto às transferências realizadas via acordo, quanto SCCs e BCRs. (BRYANT, 2023)

O novo acordo previu novas obrigações às empresas, a fim de garantir a proteção à privacidade, como, por exemplo, elaboração de acordos de processamento de dados entre controladores e operadores; acordos conjuntos de controladores entre vários controladores; obtenção do consentimento dos titulares dos dados; e o fornecimento das divulgações necessárias de acordo com o GDPR, por exemplo, políticas de privacidade de dados. (DEL SESTO; SPIES; GUO, 2023)

Similarmente ao seu predecessor, o *Data Privacy Framework* também se baseia num programa de auto certificação, sendo possível a inclusão automática de empresas que eram certificadas à época da vigência do *Privacy Shield*. (MOLE; BOARDMAN; MORRISON, 2023) Sendo este um tópico sensível, uma vez que os requisitos para auto certificação do *Privacy Shield* foram considerados insuficientes perante o TJUE.

Atualmente, o novo acordo deu uma competência e autonomia necessária para as autoridades de proteção de dados regionais, sendo que, por exemplo, o titular

---

[28] No original: "*Le texte issu de ces négociations viole la Charte des droits fondamentaux de l'Union, en raison de l'insuffisance de garanties du respect de la vie privée et familiale au regard des collectes en vrac de données personnelles, et le Règlement Général sur la Protection des Données (RGPD), en raison de l'absence de garanties d'un droit à un recours effectif et d'un accès à un tribunal impartial, de l'absence d'encadrement des décisions automatisées ou de manques de garanties relatives à la sécurité des données traitées : autant de violations de notre droit européen que je développe dans le mémoire de 33 pages (+ 283 pages d'annexes) déposé hier auprès du TJUE.*".

de dados poderia recorrer a sua autoridade para denunciar casos de incompatibilidade da transferência com os princípios do *Data Privacy*. (EUROPEAN DATA PROTECTION BOARD, p. 2)

O futuro do *Data Privacy Framework* ainda não está delineado, mas paira a dúvida sobre a efetividade deste acordo, em virtude de todos os problemas enfrentados frente às agências de investigação estadunidense. Por mais incerto que seja, Schrems, agora presidente honorário do nyob[29] (grupo militante da privacidade na UE), já indicou que planeja interpor um recurso contra a Decisão nº 2023/1795, a fim de invalidar o novo acordo. (BARCZENTEWICZ, 2023, p. 4)

[29] Nyob. Out Team. Disponível em: https://noyb.eu/en/our-team-members-and-partners. Acesso em: 5 out. 2023.

3. TRANSFERÊNCIA INTERNACIONAL DE DADOS POR MEIO DE ACORDOS BILATERAIS NA PERSPECTIVA BRASILEIRA

Esta Monografia, em seus capítulos anteriores, procurou demonstrar aspectos gerais da dinâmica das transferências internacionais e como os acordos bilaterais podem facilitar o desenvolvimento econômico, mas também os entraves que resultaram em suas anulações. Isto posto, esta última Seção visa analisar à luz da legislação brasileira a possibilidade legal de um acordo bilateral tendo o Brasil como parte, considerando aspectos anteriormente problemáticos entre UE e EUA.

3.1. Acordo bilateral como ferramenta de transferência internacional à luz da LGPD

Como delineado anteriormente, a LGPD, em seu art. 33, dispõe sobre as hipóteses previstas que autorizam transferências internacionais de dados. Dentro destas hipóteses, chama-se atenção para a autorização legal em caso de países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado (art. 33, I, da LGPD). (BRASIL, 2018)

Esta hipótese é idêntica ao embasamento legal ocorrido entre UE e EUA para a validade do *Safe Harbor*, *Privacy Shield* e *Data Privacy*. Ou seja, da mesma forma ocorrida nos acordos trazidos anteriormente, o Brasil possui a mesma hipótese legal que podem trazer à tona os mesmos problemas vivenciados nas invalidações dos acordos mencionados. Obviamente, de pronto pode-se delinear problemas no que seria um grau de proteção adequado à luz da LGPD, frente à falta de esclarecimentos pela ANPD.

Em que pese não haja um regulamento sobre transferências internacionais e decisões de adequação, a ANPD já deu os primeiros passos para regulamentar o tema. Assim, publicou, em 15 de agosto de 2023, a Consulta Pública nº 2/2023 sobre o Regulamento de Transferências Internacionais de Dados Pessoais e do modelo de Cláusulas-Padrão Contratuais. (BRASIL, 2023a)

O referido Regulamento menciona sobre a hipótese de considerar um país ou organismo internacional adequado, ou seja, que proporciona um nível equivalente de proteção de dados com base na LGPD. A avaliação dada pela ANPD, preliminarmente, consideraria os seguintes tópicos:

> I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
> II - a natureza dos dados;
> III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD;
> IV - a adoção de medidas de segurança adequadas para minimizar impactos às liberdades civis e aos direitos fundamentais dos titulares;
> V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
> VI - outras circunstâncias específicas relativas à transferência. (BRASIL, 2023a)

Ademais, chama-se atenção para a influência do RGPD na legislação brasileira, sendo que o primeiro, a partir do "Efeito Bruxelas", determinou como as legislações de proteção de dados nas maiores democracias do mundo se desenvolveriam. Neste sentido, a LGPD foi moldada pelos conceitos e princípios estabelecidos pelo RGPD, obviamente, com as particularidades inerentes ao Brasil, mas sob forte influência europeia. (DÖHMANN, 2021, p. 113)

Com uma similaridade importante, o quadro legal de proteção de dados brasileiro pode se encaminhar para um similar grau de proteção conferido pelo RGPD, não só pela sua coincidência na LGPD, mas pelo recrudescimento do cenário nacional em relação à privacidade. Por exemplo, a partir da promulgação da Lei nº 14.460/2022, a ANPD se tornou uma autarquia de natureza especial, ou seja, "a Autoridade preservará a sua autonomia técnica e decisória em relação à administração pública direta e, assim como as demais autarquias, terá gestão administrativa e financeira descentralizadas". (BRASIL, 2022c)

Ao tornar a ANPD uma autarquia especial, evidentemente, o Brasil focou no futuro ao considerar que o artigo 45, nº 2, b, do RGPD[30], dispõe que a independência de uma autoridade será considerada nas decisões de adequação. A independência requerida está vinculada à autonomia da ANPD em tomar suas decisões sem nenhuma interferência externa, seja de cunho orçamentário, de aplicação ou pressão política. (COSTA, 2023, p. 306)

Indo ao encontro das práticas internacionais, a ANPD vem demonstrando um amadurecimento na sua atuação que, invariavelmente, robustece a aplicação da

[30] Neste sentido, o referido artigo menciona: "A existência e o efetivo funcionamento de uma ou mais autoridades de controlo independentes no país terceiro ou às quais esteja sujeita uma organização internacional, responsáveis por assegurar e impor o cumprimento das regras de proteção de dados, e dotadas de poderes coercitivos adequados para assistir e aconselhar os titulares dos dados no exercício dos seus direitos, e cooperar com as autoridades de controlo dos Estados-Membros; e" (CONSELHO DA EUROPA; PARLAMENTO EUROPEU, 2016)

legislação de proteção de dados no país. Além de fortalecer a cultura de proteção de dados, o Brasil vem caminhando para conciliações bilaterais no que diz respeito a aspectos econômicos, cita-se, por exemplo, o acordo de livre comércio entre o Mercosul e a UE[31], tema este que será tratado na Subseção seguinte.

Entretanto, chama-se atenção apenas para um critério que pode ser decisivo em eventual decisão de adequação da UE em relação ao Brasil: o Projeto de Lei de Liberdade, Responsabilidade e Transparência na Internet, também conhecido como Projeto de Lei das Fake News (PL 2630/2020). O art. 54, do PL, que altera o art. 13, do MCI, dispõe que as autoridades poderão requerer que as plataformas digitais disponibilizem acesso a dados mediante decisão judicial.[32] A problemática se instala a partir da falta de finalidade da nova disposição, por exemplo, para fins de segurança nacional, podendo, assim, esbarrar nos ditames perseguidos pelo RGPD e encontrar os mesmos problemas ventilados nos casos Schrems. (BRASIL, 2023b)

Em que pese a problemática, vê-se que o Brasil pode ser um agente importante para integrar este novo mundo de um livre fluxo transfronteiriço de dados. A proximidade da LGPD com o RGPD é um fator que facilita este tema, uma vez que os padrões globais a consideram como um norte a ser seguido. Isto posto, faz-se necessário delinear, a partir dos fundamentos que levaram a invalidação dos acordos entre UE e EUA, preocupações legítimas que devem ser endereçadas em eventual acordo bilateral brasileiro.

3.2. Conteúdo mínimo a partir da experiência Schrems

A partir da experiência delineada na UE e EUA, vê-se que elementos centrais gravitam em torno da invalidação de acordos bilaterais que envolvam o livre fluxo de

---

[31] CNN. **Mercosul apresenta resposta às demandas da União Europeia para acordo de livre comércio**. Disponível em: https://www.cnnbrasil.com.br/internacional/mercosul-apresenta-resposta-as-demandas-da-uniao-europeia-para-acordo-de-livre-comercio/. Acesso em: 5 out. 2023.

[32] Neste sentido: “Art. 54. Os incisos VI e VIII do artigo 5o, o art. 13 e o art. 15, todos da Lei no 12.965, de 23 de abril de 2014, passam a vigorar com as seguintes redações: [...] Art. 13 [...] § 2o A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão, de acesso a aplicações de internet, dados pessoais cadastrais ou outras informações de identificação do usuário ou do terminal relacionadas ao registro de acesso à aplicação existente sejam guardados, inclusive por prazo superior ao previsto no caput, observado o disposto nos §§ 3o e 4o do art. 13.§ 3o Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo, e a disponibilização de dados cadastrais deverá observar o art. 10, § 3o, desta Lei”. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334&filename=PRLP+1+%3D%3E+PL+2630/2020. Acesso em: 8 out. 2023.

dados, sendo eles: acesso aos dados por serviços de inteligência; exercício dos direitos dos titulares de dados; supervisão e reparação; e limitação da finalidade.

O acesso aos dados pessoais transferidos internacionalmente por serviços de inteligência esteve no centro gravitacional da disputa de Schrems contra o Facebook Irlanda. Por isso, o primeiro aspecto abordado deve considerar que não exista exceção legal para que o governo possa coletar dados massivamente, mesmo que em prol da segurança nacional. Por óbvio, este tema adentra um terreno espinhoso de soberania nacional, entretanto, não é descabido pensar que o princípio da necessidade, previsto na LGPD, seja aplicado.

O princípio da necessidade vai demonstrar que o tratamento de dados pessoais seja o mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados. (BRASIL, 2018) Portanto, não se pugna pela impossibilidade deste tipo de tratamento de dados por agências de segurança, mas sim dentro de ditames legais e razoáveis, inclusive, com a possibilidade de criação de um organismo comum às partes que tenha poder decisivo sobre cada solicitação de acesso.

Em que pese o art. 4º, III, a, da LGPD, excetue a aplicação da legislação de proteção de dados no caso de tratamento de dados para fins de segurança pública, é importante delinear que acordos que previam a exceção por completo nestes casos estiveram fadados ao fracasso. (BRASIL, 2018) Deve-se buscar uma interpretação harmônica de princípios para que casos de exacerbação por parte do Estado não ocorram, sendo que mecanismos de salvaguarda podem auxiliar na proteção da privacidade dos titulares.

Considerando o exposto anteriormente, precisa-se balizar as necessidades destes mecanismos com a realidade brasileira. No Brasil, o acesso a dados pessoais tratados por empresas, geralmente, se dá apenas a partir de requerimentos judiciais, sendo possível a garantia do contraditório e ampla defesa, dentro dos ditames legais (e.g. pode-se utilizar a via do MLAT para acesso a dados pessoais em investigações de matéria penal). O Poder Judiciário, por sua vez, seria o responsável por ponderar as requisições, ainda que para fins de segurança nacional.

Os mecanismos de salvaguardas que podem limitar a atuação potestativa estatal também estão inseridos no âmbito do exercício dos direitos dos titulares de dados pessoais. A criação de mecanismos de transparência que permitam que o titular

escolha é de suma importância, como, por exemplo, a adoção do *opt out* em caso de oposição ao tratamento de dados.

Maneiras de garantir a autodeterminação informativa vão ao encontro do exercício dos direitos, mesmo diante de sua perda em meio às assimetrias do mercado informacional e a mística capacidade de controle dos seus dados. (BIONI, 2021, p. 197) Portanto, considerações acerca da capacidade do titular concordar com as transferências internacionais para determinados países é de suma importância e devem ser previstas nos mecanismos de transferência.

Além disso, os titulares devem levar a cabo seus direitos de acesso, revisão, retificação e até exclusão de seus dados pessoais, conforme determina o art. 18 da LGPD. Logo, deve-se garantir que os titulares tenham conhecimento da finalidade da coleta e da eventual utilização de seus dados, inclusive, como uma medida de garantia de direitos fundamentais. Neste sentido, ensina Ruaro e Sarlet (2021, p. 202): “Deve-se igualmente relembrar o direito ao conhecimento da finalidade da coleta e da eventual utilização dos dados para arrolar o direito à retificação e, a depender do caso, de exclusão de dados pessoais armazenados em banco de dados”.

Os direitos dos titulares devem ser exercidos para garantir o controle sobre seus dados pessoais. Importante ressaltar, a criação de mecanismos que viabilizem a resolução de conflitos deve ser considerada, tal qual o *Privacy Shield Panel*, que inclusive garanta o direito recursal do titular em caso de negativas no exercício de seus direitos, consoante ao art. 5º, LV, da Constituição Federal. (BRASIL, 1988)

A criação de um órgão supranacional que abarque representantes de ambas as partes é essencial para uma melhor prestação de contas e responsabilidade, pois garante que os termos do acordo estejam sendo cumpridos por ambas as partes. Este órgão deve ser capaz de receber denúncias e petições de titulares para avaliações dos termos das transferências de determinadas empresas, sem, contudo, excluir a competência das autoridades de proteção dados nacionais na investigação e fiscalização dos agentes de tratamento.

A possibilidade que o titular de dados seja ressarcido por danos causados pelas transferências internacionais indevidas ou sem as salvaguardas necessárias deve fazer parte do acordo. Os mecanismos de reparação estão em consonância com a legislação brasileira de proteção de dados, inclusive, com o regime de responsabilidade contido no art. 42, da LGPD. (BRASIL, 2018)

Por fim, mas não menos importante, deve-se delinear um contexto muito específico para a finalidade do tratamento originalmente informado ao titular. O tratamento posterior incompatível com aquele informado ao titular deve ser vedado, nos termos do art. 6º, I, da LGPD. (BRASIL, 2018) Deve-se garantir que os dados sejam tratados com uma finalidade específica e limitados a estrita necessidade para atingimento da finalidade.

Uma finalidade posterior incompatível com aquele originária não deve ser concebida. Entretanto, caso haja um novo tratamento para uma nova finalidade, o titular de dados deve ser informado para, assim, exercer o controle direto e assertivo na concordância ou discordância com os novos termos. Isto pois, conforme ensina Mendes e Fonseca (2021, p. 94), “o titular de dados se encontra no centro do processo decisório acerca do que é feito com seus dados pessoais”.

Neste sentido, os dados pessoais tratados só podem ser realizados apenas para a finalidade para a qual foram coletados, em observância estrita ao princípio da finalidade. Delimitações em relação à finalidade contêm uma importância intrínseca à própria proteção de dados, isto pois, nas palavras de Döhmann (2021, p. 121), “A finalidade define e limita o tratamento de dados a essa finalidade. Caso os dados sejam tratados em um passo adicional ou sejam, mais tarde, tratados para uma outra finalidade, faz-se necessária uma justificativa nova e à parte”.

3.3. Caminho para o futuro do livre fluxo de dados por meio do Mercosul

O Mercosul, bloco econômico formado por Brasil, Argentina, Paraguai e Uruguai, em 28 de janeiro de 2021, aprovou o Acordo sobre Comércio Eletrônico por meio da Decisão MERCOSUL/CMC/DEC nº 15/20 que, em conjunto, visam facilitar e promover mecanismos de intercâmbio por meio de novas tecnologias. (MERCOSUL, 2021, p. 2)

O art. 6º do referido acordo traz à tona o tema da proteção de dados no livre comércio intrabloco do Mercosul. Nestes termos, o acordo menciona a importância da proteção de dados no comércio entre os países e, especialmente no art. 6º (7), menciona:

> As partes comprometem-se a aplicar aos dados pessoais que recebam de outra Parte um nível adequado de proteção por meio de regra geral ou regulamento autônomo específico ou por acordos mútuos, gerais ou

> específicos ou em instrumentos internacionais mais amplos, permitindo a execução de contratos ou auto-regulamentação para o setor privado. (MERCOSUL, 2021, p. 5-6)

Sendo que o art. 7º trata sobre a transferência transfronteiriça de informações por meios eletrônicos, determinando que o art. 6º (7) seja cumprido nos casos de transferências internacionais, sendo, especialmente, permitas as transferências de cunho comercial. Em outras palavras, o nível de proteção adequado de dados deve ser garantido, entretanto, para que isso possa efetivamente ser aplicado, deve-se existir instrumentos específicos para esta finalidade.

O acordo visa eliminar barreiras injustificadas e garantir o direito dos titulares de dados dos países integrantes do Mercosul, menciona-se, por exemplo, que as partes arbitrarão os meios necessários para estabelecer medidas comuns de proteção de dados pessoais e sua livre circulação no bloco. A tentativa é honesta e tenta colocar os países integrantes do bloco mais importante da América do Sul em evidência e a frente dos debates do século. (COSTA, 2023, p. 299)

Para além do acordo intrabloco, é importante ressaltar as tratativas do Mercosul com a UE para a finalização de um acordo de livre comércio. Em conjunto, os blocos correspondem à 25% da economia mundial e um mercado com 780 milhões de habitantes[33], caso o acordo venha a ser entabulado efetivamente, isto constituiria uma das maiores áreas de livre comércio do mundo. (COSTA, 2023, p. 300)

Neste sentido, é importante vislumbrar o papel das transferências internacionais no acordo de livre comércio Mercosul-UE, isto pois, espera-se que a economia de dados represente, até 2025, aproximadamente 5,4% do PIB da UE que equivaleria à €544 bilhões.[34] A UE, desde a Diretiva nº 95/46/CE, atuou na proteção de dados de seus cidadãos e o Mercosul, pela primeira vez, aprovou um acordo

---

[33] Nos termos abordados pelo Siscomex sobre o Acordo Mercosul – UE: "*O acordo comercial com a UE constituirá uma das maiores áreas de livre comércio do mundo ao integrar um mercado de 780 milhões de habitantes e aproximadamente a quarta parte do PIB global.*". Disponível em: https://www.gov.br/siscomex/pt-br/acordos-comerciais/mercosul-uniao-europeia. Acesso em: 6 out. 2023.

[34] Os dados são abordados pelo comentário do Vice-Presidente para Mercados Digitais da UE: "*Vice-President for the Digital Single Market Andrus Ansip said: "By 2025 the data economy of the EU27 is likely to provide 5.4% of its GDP, equivalent to €544 billion. However, that huge potential is limited if data cannot move freely. By removing forced data localisation restrictions, we give more people and businesses the chance to make the most out of data and its opportunities. Today's guidance will now give full clarity on how free-flow of non-personal data interacts with our strong personal data protection rules.*". Disponível em: https://ec.europa.eu/commission/presscorner/detail/pt/IP_19_2749. Acesso em: 6 out. 2023.

intrabloco de proteção de dados, vislumbrando, portanto, a importância da proteção de dados no desenvolvimento da sociedade. (COSTA, 2023, p. 300)

Assim, pensar que o acordo de livre comércio entre UE e Mercosul envolva transferências internacionais de dados é o caminho necessário para a ampliação dos benefícios da criação desta zona comercial. O comprometimento do Mercosul com a proteção de dados é uma sinalização relevante que, em algum momento, poderá levar à uma decisão de adequação do bloco em relação à UE.

Além disso, é válido analisar que uma decisão de adequação do Mercosul representaria uma inovação em relação à dois membros apenas: Brasil e Paraguai. Isto pois, Argentina e Uruguai já foram considerados adequados pela UE para fins de transferências internacionais de dados[35]. (COSTA, 2023, p. 301) Neste sentido, à título exemplificativo, demonstra-se que o acordo de livre comércio entre UE e Japão andou de mãos dadas à decisão de adequação do país asiático, portanto, é crível presumir que uma decisão de adequação do Mercosul poderia ser um resultado esperado para a UE.

[35] Neste sentido, a Comissão Européia dispõe: "*The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland , the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay as providing adequate protection.*". Disponível em: https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,commercial%20organisations%20participating%20in%20the. Acesso em: 8 out. 2023.

CONSIDERAÇÕES FINAIS

As transferências internacionais de dados pessoais são condições *sine qua non* para o desenvolvimento e intercâmbio livre de dados. Como demonstrado nesta Monografia, as transferências estão intimamente ligadas à comercialização de dados na sociedade da informação. Imaginar que um dado pessoal coletado pode, ao mesmo tempo, estar sendo transferido internacionalmente demonstra como a dinâmica das transferências são abordadas e sua importância.

Como qualquer outro tema que envolva proteção de dados, as transferências internacionais encontram um obstáculo difícil quando se fala em fronteiras digitais entre países com diferentes sistemas legais de proteção à privacidade. Esta Monografia procurou explorar, de maneira acentuada, o sistema brasileiro e o europeu.

Como diferentes sistemas legais interagem e como diferentes mecanismos são utilizados para harmonização legal é a conclusão que esta Monografia quis chegar. A partir disso, em uma análise dos acordos bilaterais firmados entre UE e EUA, pode-se identificar problemas relacionados à soberania nacional, em especial, à segurança pública. O acesso à dados de cidadãos europeus por agências estadunidenses de inteligência é o ponto fulcral na discussão do tema.

Como pôde-se ver, o TJUE foi uma instância judicial importante na interpretação das leis de proteção de dados da UE e como, na prática, os estadunidenses tiveram dificuldades para harmonizar o seu sistema com o europeu, uma vez que fundados em raízes distintas. A dificuldade de se entabular um acordo entre gigantes demonstra a complexidade do assunto, entretanto, lograram êxito em três negociações, mesmo que, mais tarde, duas tenham sido em vão.

Portanto, analisar a eficácia de acordos bilaterais como mecanismos de transferências internacionais pôde transparecer que são efetivos, por mais que tenham problemas de harmonização legal. Neste sentido, aguardar uma decisão de adequação pode ser um caminho custoso que um tempo desnecessário frente à urgência do desenvolvimento econômico, principalmente, em países do sul global.

Vê-se, assim, que acordos bilaterais são ferramentas necessárias para garantir proteção aos dados dos titulares e privacidade. Como delineado no desenvolvimento desta Monografia, a partir da experiência Schrems, um conteúdo mínimo deve ser entendido como necessário nas salvaguardas dos titulares de dados,

sendo eles: acesso aos dados por serviços de inteligência, exercício dos direitos de titulares, supervisão e reparação, e limitação da finalidade.

Isto posto, do ponto de vista legal, a legislação brasileira comporta os mecanismos adotados, por exemplo, pela UE e EUA, sendo a LGPD clara neste aspecto. Neste sentido, um acordo bilateral colocaria o Brasil num lugar de relevância econômico, uma vez que sua população é a 7ª maior do mundo, tendo uma produção massiva de dados a cada segundo.

Para isto, o Brasil precisaria concluir algumas considerações acerca de seu amadurecimento, por exemplo, regular como se dão as transferências internacionais. Todavia, vislumbra-se um encaminhamento para um futuro em que o Brasil ganhará seu lugar frente ao desenvolvimento tecnológico e social. Ademais, este caminho pode ser encurtado por meio do Mercosul, caso o acordo de livre comércio entre UE e bloco sul-americano fosse concluído. Para o sul global, decisões de harmonização simples do *framework* legal entre os países que fazem parte do Mercosul é um espaço relevante e importante a ser considerado.

REFERÊNCIAS BIBLIOGRÁFICAS

BARCZENTEWICZ, Mikolaj. **Schrems III: Gauging the Validity of the GDPR Adequacy Decision for the United States**. Portland: International Center for Law & Economics, 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4585431. Acesso em: 5 out. 2023.

BERTOLDI, Chiara. **The New European Commission Decision on Standard Contractual Clauses: A System Reform?.** Vol. 6, nº 3, p. 1363-1365. [s.l]: European Papers, 2021. Disponível em: https://www.europeanpapers.eu/en/europeanforum/new-european-commission-decision-standard-contractual-clauses-system-reform#_ftn2. Acesso em: 17 jul. 2023.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: a função e os limites do consentimento**. 3ª ed. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530994105/epubcfi/6/10%5B%3Bvnd.vst.idref%3Dcopyright%5D!/4/26/4/2/2/2. Acesso em: 5 out. 2023.

BRADFORD, Anu. **The Brussels Effect**. Nº 533. Nova Iorque: Columbia Law and Economics Working Paper, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2770634. Acesso em: 25 jun. 2023.

BRANDEIS, Louis D.; WARREN, Samuel D. **The right to privacy**. Vol. 4, nº 5. Boston: The Harvard Law Review Association, 1890. Disponível em: https://www.jstor.org/stable/1321160. Acesso em: 18 jun. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Portaria ANPD nº 35, de 4 de novembro de 2022**. Torna pública a Agenda Regulatória para o biênio 2023-2024. Brasília: [s.n.], 2022a. Disponível em: https://www.in.gov.br/en/web/dou/-/portaria-anpd-n-35-de-4-de-novembro-de-2022-442057885. Acesso em: 17 jul. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: [s.n.], 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 jul. 2023.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011 (LAI)**. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Brasília: [s.n.], 2011. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1. Acesso em: 17 jul. 2023.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília: [s.n.], 2014. Disponível

em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 5 jul. 2023.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: [s.n.], 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 5 de jul. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Nota Técnica nº 20/2022/CGN/ANPD**. Proposta de realização de Tomada de Subsídios para regulamentação de transferência internacional de dados pessoais, nos termos dos arts. 33 e 35 da LGPD da Lei no 13.709, de 14 de agosto de 2018. Brasília: [s.n.], 2022b. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000968_2021_06-nota-tecnica.pdf. Acesso em: 17 jul. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Congresso Nacional promulga a Lei nº 14.460 que transforma a ANPD em autarquia de natureza especial**. Brasília: site ANPD, 2022c. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/congresso-nacional-promulga-a-lei-no-14-460-que-transforma-a-anpd-em-autarquia-de-natureza-especial. Acesso em: 5 out. 2023.

BRASIL. Autoridade Nacional de Proteção de Dados. **Consulta Pública Nº 2, de 14 de agosto de 2023**. Brasília: Diário Oficial da União, 2023a.

BRASIL. Senado Federal. **Substitutivo do Projeto de Lei nº 2630/2020**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília: [s.n.], 2023b. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334&filename=PRLP+1+%3D%3E+PL+2630/2020. Acesso em: 8 out. 2023.

BRYANT, Jennifer. **EU-US Data Privacy Framework adopted, what now?**. [s.l.]: IAPP, 2023. Disponível em: https://iapp.org/news/a/eu-us-data-privacy-framework-adopted-what-now/. Acesso em: 4 out. 2023.

CONSELHO DA EUROPA. **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**, 1981. Disponível em: https://rm.coe.int/1680078b37. Acesso em: 25 jun. 2023.

CONSELHO DA EUROPA; PARLAMENTO EUROPEU. **Regulation (EU) 2016/279 – General Data Protection Regulation (GDPR)**. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679&qid=1689553254770. Acesso em: 16 jul. 2023.

COSTA, Janaina. **Acordo comercial internacional UE- MERCOSUL: uma oportunidade para a criação da maior zona de livre fluxo de dados do mundo?**. In: BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (Coords.). Plataformas digitais e proteção de dados pessoais. Rio de Janeiro: Instituto de Tecnologia e Sociedade do

Rio, 2023. Disponível em: https://itsrio.org/wp-content/uploads/2023/09/20230929_Livro_Pos_ITS-UERJ_Plataformas-digitais-protecao-de-dados_COMPLETO.pdf. Acesso em: 5 out. 2023.

DEL SESTO, Ronald W.; SPIES, Axel; GUO, Jiazhen. **How to comply with the new EU-US Data Privacy Framework**. [s.l]: [s.n], 2023. Disponível em: https://www.morganlewis.com/pubs/2023/07/how-to-comply-with-the-new-eu-us-data-privacy-framework. Acesso em: 4 out. 2023.

DÖHMANN, Indra Spiecker Gen. **A proteção de dados pessoais sob o Regulamento Geral de Proteção de Dados da União Europeia**. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/ - /books/9788530992200/ . Acesso em: 5 out. 2023.

DONEDA, Danilo. **Panorama histórico da proteção de dados pessoais**. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/ - /books/9788530992200/ . Acesso em: 5 jul. 2023.

ERNST, Florian; FRISCHE, Patrick. **Industry 4.0 / Industrial Internet of Things - Related Technologies and Requirements for a Successful Digital Transformation: An Investigation of Manufacturing Businesses Worldwide**. [s.l.]: [s.n.], 2015. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2698137#paper-references-widget. Acesso em: 19 out. 2023.

ESTADÃO. **O que Snowden revelou**. [2013]. Disponível em: https://infograficos.estadao.com.br/especiais/snowden/revelacoes.html#:~:text=O%20Prism%20foi%20criado%20para,governo%20do%20presidente%20George%20W. Acesso em: 2 de out. 2023.

ESTADOS UNIDOS DA AMÉRICA. **H.R. 8152 - American Data Privacy and Protection Act, of June 21, 2022**. To provide consumers with foundational data privacy rights, create strong oversight mechanisms, and establish meaningful enforcement. Disponível em: https://www.congress.gov/bill/117th-congress/house-bill/8152/text. Acesso em: 25 jun. 2023.

ESTADO UNIDOS DA AMÉRICA. The White House. **Executive Order On Enhancing Safeguards For United States Signals Intelligence Activities**. 2023. Disponível em: https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/. Acesso em: 4 out. 2023.

EUROPEAN DATA PROTECTION BOARD. **Information note on data transfers under the GDPR to the United States after the adoption of the adequacy decision on 10 July 2023**. Bruxelas: [s.n], 2023. Disponível em: https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf. Acesso em: 4 out. 2023.

GARCÍA-CUEVAS ROQUE, Elena. **Las transferencias internacionales de datos y las libertades individuales: un acercamiento a las normas de protección de datos**. Vol. 6, nº 2, p. 171-193. [s.l]: Estudios de Deusto, 2014.

JESUS, Damásio E.; OLIVEIRA, José Antônio M. **Marco Civil da Internet: comentários à Lei n. 12.965, de 23 de abril de 2014**. 1ª ed. São Paulo: Editora Saraiva, 2014. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502203200/. Acesso em: 05 jul. 2023.

KUNER, Christopher. **An International Legal Framework for Data Protection: Issues and Prospects**. Vol. 25. P. 307-317. [s.l]: Computer Law & Security Review, 2009. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1443802. Acesso em: 09 jul. 2023.

KUNER, Christopher. **Reality and Illusion in EU Data Transfer Regulation Post Schrems**. Vol. 18, nº 4, p. 881-918. [s.l.]: German Law Journal, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2732346. Acesso em: 2 out. 2023.

KUNER, Christopher. **Developing an Adequate Legal Framework for International Data Transfers**. p. 263-273. [s.l.]: Springer Science+Business Media B.V., 2009. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1464323. Acesso em : 2 out. 2023.

LATOMBE, Philippe. **Communiqué de presse**. [s.l]: [s.n], 2023. Disponível em: https://www.politico.eu/wp-content/uploads/2023/09/07/4_6039685923346583457.pdf. Acesso em: 4 out. 2023

LEONARDI, Marcel. **Transferência internacional de dados pessoais**. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/ - /books/9788530992200/ . Acesso em: 12 jul. 2023.

MENDES, Laura Schertel; FONSECA, Gabriel Campos S. **Proteção de dados para além do consentimento: tendências de materialização**. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/ - /books/9788530992200/ . Acesso em: 5 out. 2023.

MERCOSUL. Consejo del Mercado Común. **Acordo sobre Comércio Eletrônico do Mercosul**. [s.l.]: [s.n], 2021. Disponível em: https://normas.mercosur.int/simfiles/normativas/82753_DEC_015-2020_PT_Acordo%20Comercio%20Eletronico.pdf. Acesso em: 6 out. 2023.

MOLE, Ariane; BOARDMAN, Ruth; MORRISON, Robbie. **Third times a charm? The new EU-US Data Privacy Framework**. [s.l]: [s.n.], 2023. Disponível em: https://www.twobirds.com/en/insights/2023/global/third-times-a-charm-the-new-eu-us-data-privacy-framework. Acesso em: 4 out. 2023.

NI LOIDEAIN, Nora. **The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law.** Vol. 19, nº 8. Cambridge: Journal of Internet Law, 2016. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2734698. Acesso em: 01 out. 2023.

MANYIKA, JAMES et al. **Digital Globalization: the new era of global flows**. [s.l]: McKinsey Global Institute, 2016. Disponível em: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.pdf. Acesso em: 09 jul. 2023.

MARQUES, Fernanda M.; AQUINO, Theófilo M. de. **O regime de transferência internacional de dados da LGPD: delineando as opções regulatórias em jogo**. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/ -/books/9788530992200/ . Acesso em: 05 jul. 2023.

MUCHIUTI, Marília Machado. **Do RGPD à LGPD: Difusão internacional de normas e o caso das regulamentações de proteção de dados pessoas**. São Paulo: [s.n.], 2022. Disponível em: https://repositorio.pucsp.br/jspui/handle/handle/29644. Acesso em: 25 jun. 2023.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 7 jun. 2023.

PALMER, Michael. **ANA Marketing Maestros: Data is the New Oil**. 2006. Disponível em: https://ana.blogs.com/maestros/2006/11/data_is_the_new.html. Acesso em: 7 jun. 2023.

PELEGRINI, Rafael T.; PELEGRINI, Ramon T. **Marco Civil: Liberdade e o Futuro da Internet**. Vol. 6, nº 12, p. 265-270. Florianópolis: Tempo e Argumento, 2014. Disponível em: https://revistas.udesc.br/index.php/tempo/article/view/2175180306122014265. Acesso em: 25 jun. 2023.

REIDENBERG, Joel R. **Lex Informatica: The formulation of Information Policy Rules through technology**. Vol. 76, nº 3, p. 553-593. Texas: Texas Law Review, 1998. Disponível em: https://ir.lawnet.fordham.edu/faculty_scholarship/42/. Acesso em: 17 jul. 2023.

RUARO, Regina Linden; SARLET, Gabrielle Bezerra S. **O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (LGPD) – Lei 13.709/2018**. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/ - /books/9788530992200/ . Acesso em: 5 jul. 2023.

SANTOS, Luiza Mendonça da S. B.; VERONESE, Alexandre. **Padrões de conformidade nacionais de proteção de dados pessoais: anotações na perspectiva de compliance após a invalidação do Privacy Shield firmado entre os Estados Unidos da América e a União Europeia**. In: CUEVA, Ricardo Villas B (coord.); FRAZÃO, Ana (coord.). Compliance e Política de Proteção de Dados. São Paulo: Thomson Reuters Brasil, 2021.

SCHWARTZ, Paul M. **The EU-US privacy collision: a turn to institutions and procedures**. Vol. 126, p. 1966-2009. Boston: Harvard Law Review, 2013. Disponível em: https://harvardlawreview.org/print/vol-126/the-eu-u-s-privacy-collision-a-turn-to-institutions-and-procedures/. Acesso em: 27 set. 2023.

SCHWARTZ, Paul M.; PEIFER, Karl-Nikolaus. **Transatlantic data privacy law**. Vol. 106, nº 1, p. 115-179. [s.l.]: The Georgetown Law Journal, 2017. Disponível em: https://www.law.georgetown.edu/georgetown-law-journal/wp-content/uploads/sites/26/2019/10/Transatlantic-Data-Privacy-Law_Schwartz-and-Peifer.pdf. Acesso em: 27 set. 2023.

SRIVASTAVA, Prachi; SINGH, Rupinder; SONKAR, Sharad Kumar. **Mapping of Research Output in the field of Big Data Analytics: Scientometric Study**. 6378 ed. Nebraska: Library Philosophy and Practice, 2021. Disponível em: https://digitalcommons.unl.edu/libphilprac/6378. Acesso em: 18 jun. 2023.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M**. Lei Geral de Proteção de Dados Pessoais: comentado artigo por artigo**. 4ª ed. São Paulo: Editora Saraiva, 2022. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 12 jul. 2023.

UNIÃO EUROPEIA. Comissão das Comunidades Europeias. **2000/520/CE**: Decisão da Comissão de 26 de Julho de 2000 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho e relativa ao nível de protecção assegurado pelos princípios de «porto seguro» e pelas respectivas questões mais frequentes (FAQ) emitidos pelo Department of Commerce dos Estados Unidos da América Decisão. Bruxelas: Jornal Oficial da União Europeia, 2000. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:02000D0520-20000825. Acesso em: 01 out. 2023.

UNIÃO EUROPEIA. Comissão Europeia. **2016/1250**: Decisão de Execução da Comissão de 12 de julho de 2016 relativa ao nível de proteção assegurado pelo Escudo de Proteção da Privacidade UE-EUA, com fundamento na Diretiva 95/46/CE do Parlamento Europeu e do Conselho. 2016. Bruxelas: Jornal Oficial da União Europeia, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016D1250&qid=1696299969427. Acesso em 3 out. 2023.

UNIÃO EUROPEIA. Comitê Europeu De Proteção De Dados. **Recommendations 01/2021 on the adequacy referential under the Law Enforcement Directive**. Bruxelas: European Data Protection Board, 2021. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/recommendations012021onart.36led.pdf_en.pdf. Acesso em: 17 jul. 2023.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. **Acórdão (Grande Seção) de 6 de outubro de 2015**. Processo C-362/14. Luxemburgo: [s.n.], 2015. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62014CJ0362&qid=1696292787731. Acesso em: 2 out. 2023.

UNIÃO EUROPEIA. Tribunal de Justiça da União Europeia. **Acórdão (Grande Seção) de 16 de julho de 2020**. Processo C-311/19. Luxemburgo: [s.n.], 2020. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:62018CJ0311&qid=1696466060668. Acesso em: 4 out. 2023.

UNIÃO EUROPEIA. Comissão Europeia. **2023/1795**: Decisão da Comissão de 10 de julho de 2023 nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho sobre a adequação do nível de proteção dos dados pessoais no âmbito Quadro de Privacidade de Dados UE-EUA. Bruxelas: Jornal Oficial da União Europeia, 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32023D1795&qid=1696470363117. Acesso em: 4 out. 2023.

VÉLIZ, Carissa. **Privacidade é poder: por que e como você deveria retomar o controle de seus dados**. São Paulo: Contracorrente, 2021.

VERONESE, Alexandre. **Transferências Internacionais de Dados Pessoais: o debate transatlântico norte e sua repercussão na América Latina e no Brasi**l. In: BIONI, Bruno *et al*. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021. Disponível em: https://integrada.minhabiblioteca.com.br/ -/books/9788530992200/ . Acesso em: 1 out. 2023.