UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS JURÍDICAS
FACULDADE DE DIREITO DO RECIFE
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO

EDNALDO RODRIGUES DE ALMEIDA FILHO

O REGIME JURÍDICO INTERNACIONAL DA PROTEÇÃO DE DADOS PESSOAIS E SEUS REFLEXOS NO COMÉRCIO INTERNACIONAL

Recife PE
2020

EDNALDO RODRIGUES DE ALMEIDA FILHO

O REGIME JURÍDICO INTERNACIONAL DA PROTEÇÃO DE DADOS PESSOAIS E SEUS REFLEXOS NO COMÉRCIO INTERNACIONAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito do Centro de Ciências Jurídicas, Faculdade de Direito do Recife da Universidade Federal de Pernambuco, como parte dos requisitos parciais para obtenção do título de Mestre em Direito.
Área de Concentração: Direito Internacional.

Orientadora: Profª. Drª. Eugênia Cristina Nilsen Ribeiro Barza

Recife PE
2020

Catalogação na fonte
Bibliotecário Jefferson Luiz Alves Nazareno, CRB-4/1758

A447r Almeida Filho, Ednaldo Rodrigues de.
O regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional / Ednaldo Rodrigues de Almeida Filho – Recife, 2020.
133 f.

Orientadora: Profa. Dra. Eugênia Cristina Nilsen Ribeiro Barza.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. Centro de Ciências Jurídicas. Programa de Pós-Graduação em Direito, 2020.

Inclui referências.

1. Economia digital. 2. Dados pessoais. 3. Transferência internacional de dados. 4. Comércio internacional. I. Barza, Eugênia Cristina Nilsen Ribeiro. (Orientadora). II. Título.

341.75 CDD (22. ed.) UFPE (BSCCJ 2021-03)

FICHA DE APROVAÇÃO

EDNALDO RODRIGUES DE ALMEIDA FILHO

O REGIME JURÍDICO INTERNACIONAL DA PROTEÇÃO DE DADOS PESSOAIS E SEUS REFLEXOS NO COMÉRCIO INTERNACIONAL

Dissertação apresentada ao Programa de Pós-Graduação em Direito do Centro de Ciências Jurídicas, Faculdade de Direito do Recife da Universidade Federal de Pernambuco, como parte dos requisitos parciais para obtenção do título de Mestre em Direito.
Área de Concentração: Direito Internacional.

Aprovada em: 05/02/2020

BANCA EXAMINADORA

_____

Profª. Drª. Eugênia Cristina Nilsen Ribeiro Barza (Orientadora)
Universidade Federal de Pernambuco

_____

Profº. Dr. Aurélio Agostinho da Bôaviagem (Examinador Interno)
Universidade Federal de Pernambuco

_____

Profª. Drª. Cynara de Barros Costa (1ª Examinadora Externa)
Universidade Estadual da Paraíba

_____

Profª. Drª. Rogéria Gladys Sales Guerra (2ª Examinadora Externa)
Universidade Católica de Pernambuco

O sucesso é uma jornada, não um destino.
A ação é geralmente mais importante que o resultado.
Nem todo mundo pode ser o número 1.
(Arthur Robert Ashe, tenista norte-americano)

AGRADECIMENTOS

À minha família e amigos, pelo apoio incondicional;
A todo corpo docente e funcionários do PPGD/FDR, pela entrega e dedicação diárias;
Aos colegas de pós-graduação, pelas valiosas discussões que muito contribuíram para a elaboração deste trabalho.

RESUMO

A digitalização da economia facilitou o comércio tradicional e possibilitou a criação de novos modelos de negócios, cada vez mais dependentes do acesso à internet e da capacidade de coleta, armazenamento, processamento e movimentação de dados pessoais através das fronteiras nacionais. Os últimos anos testemunharam um aumento nas discussões relacionadas à proteção e transferência internacional de dados. Os fluxos internacionais de dados deram origem a uma série de preocupações de governos e cidadãos sobre alguns dos efeitos de tanta informação sendo coletada e usada, geralmente sem o conhecimento dos titulares dos dados. De um lado, essas novas questões refletem preocupações regulatórias na área da privacidade e segurança de dados. Por outro, elas surgem da divergência de interesses e políticas das principais economias digitais. Embora as transferências internacionais de dados sejam essenciais para o comércio internacional, vários países têm proibido ou procurado restringir esses fluxos, seja, afetando o comércio no processo. A futura estrutura para a governança do comércio digital e da proteção de dados ainda é uma questão em aberto, com inexistindo unanimidade quanto ao caminho a seguir. A busca por uma regulamentação de proteção de dados equilibrada, flexível e compatível se tornou um objetivo urgente. Para obter uma proteção adequada que permita inovações e facilite o comércio, é essencial continuar o diálogo nacional, regional e global entre governos, organismos internacionais e sociedade civil. Através de uma revisão da literatura, o presente trabalho analisa o impacto do fluxo internacional de dados no comércio internacional. Após contextualizar o atual estágio da globalização e da digitalização da economia, discute os principais aspectos da proteção e transferência internacional de dados, concluindo com o debate acerca das diretrizes para uma regulação global da matéria.

Palavras chaves: Economia Digital. Dados Pessoais. Transferência Internacional de Dados. Comércio Internacional.

ABSTRACT

The digitization of the economy has facilitated traditional commerce and enabled the creation of new business models, increasingly dependent on internet access and the ability to collect, store, process and move personal data across national borders. The past few years have seen an increase in discussions related to international data protection and transfer. International data flows have given rise to a number of concerns from governments and citizens about some of the effects of so much information being collected and used, usually without the knowledge of the data subjects. On the one hand, these new issues reflect regulatory concerns in the area of data privacy and security. On the other hand, they arise from the divergence of interests and policies of the main digital economies. Although international data transfers are essential for international trade, several countries have prohibited or sought to restrict these flows, that is, affecting trade in the process. The future structure for the governance of digital commerce and data protection is still an open question, with unanimity as to the way forward. The search for balanced, flexible and compatible data protection regulations has become an urgent objective. In order to obtain adequate protection that allows for innovations and facilitates trade, it is essential to continue the national, regional and global dialogue between governments, international organizations and civil society. Through a literature review, this work analyses the impacts of the international data flow in international trade. After contextualizing the current stage of globalization and digitalization of the economy, discuss the main aspects of international data protection and transfer, concluding with the debate about guidelines for a global regulation of the theme.

Keywords: Digital Economy. Personal Data. International Data Transfer. International Trade.

LISTA DE SIGLAS

APEC - Cooperação Econômica Ásia-Pacífico
ANPD - Autoridade Nacional de Proteção de Dados
BIRD - Banco Internacional para Reconstrução e Desenvolvimento
B2B - Business-to-business
B2C - Business to Consumer
CEDH - Convenção Europeia dos Direitos Humanos
CPC - Classificação Central de Produtos Básicos
ECOWAS - Comunidade Econômica dos Estados da África Ocidental
FMI – Fundo Monetário Internacional
GATS - Acordo Geral sobre o Comércio de Serviços
GATT - Acordo Geral de Tarifas e Comércio
GDPR - Regulamento Geral sobre a Proteção de Dados
ICANN - Internet Corporation for Assigned Names and Numbers
IEEE - Institute of Electrical and Eletronics Engineers
IETF - Internet Engineering Task Force
IOT - Internet das Coisas
IP - Protocolo Internet
ITA - Acordo sobre Tecnologia da Informação
ITU - International Telecommunications Union
LGPD - Lei Geral de Proteção de Dados Pessoais
MGI - McKinsey Global Institute
OCDE - Organização para a Cooperação e Desenvolvimento Econômico
OIC - Organização Internacional do Comércio
OMC - Organização Mundial do Comércio
ONU – Organização das Nações Unidas
PME - Pequenas e médias empresas
PIB - Produto Interno Bruto
RCV - Regras Corporativas Vinculantes
SERPRO - Serviço Federal de Processamento de Dados
TIC - Tecnologias da informação e da comunicação
TJUE - Tribunal de Justiça da União Europeia
TRIPS - Aspectos dos Direitos de Propriedade Intelectual

UNCITRAL - Comissão das Nações Unidas para o Direito Internacional do Comércio
UNCTAD - Conferência das Nações Unidas sobre Comércio e Desenvolvimento
USITC - Comissão de Comércio Internacional dos Estados Unidos
W3C - World Wide Web Consortium

SUMÁRIO

INTRODUÇÃO

O mundo está cada vez mais conectado. O desenvolvimento de atividades econômicas, políticas e sociais no mundo online tem impactado a maneira como os negócios são conduzidos e as pessoas interagem entre si, tornando a rede de conexões globais mais profunda, ampla e complexa.

Enquanto o comércio de bens e serviços e a circulação de capitas experimentaram retração desde a crise financeira de 2008, a globalização do século XXI é moldada pelos fluxos de dados, informações e conhecimentos. Esse fenômeno agora sustenta praticamente todas as transações internacionais.

A disseminação das tecnologias digitais está transformando todos os tipos de fluxos globais tradicionais - bens, serviços, capital e pessoas - e essa transformação está apenas em seus estágios iniciais. Atualmente, mais e mais pessoas em todo o mundo se envolvem em trocas instantâneas de mercadorias digitais, livros e músicas a arquivos de design que permitem a impressão 3D de objetos físicos. À medida que a infraestrutura da internet se expande, as barreiras de distância e custo que antes pareciam intransponíveis começaram a cair.

A digitalização muda a economia da globalização de várias maneiras. À medida que as plataformas digitais se tornam globais em escopo, elas estão reduzindo o custo das comunicações e transações internacionais, permitindo que as empresas se conectem com clientes e fornecedores em qualquer país.

Durante muito tempo, a globalização servia apenas às grandes empresas multinacionais, mas as plataformas reduzem a escala mínima necessária para se tornarem globais, permitindo a participação de pequenas empresas e empreendedores em todo o mundo. Como resultado, novos concorrentes podem emergir rapidamente de qualquer canto do mundo, aumentando a pressão sobre outros *players* do mercado.

A digitalização reduz os custos marginais de produção e distribuição, ampliando o acesso ao comércio global. O custo da participação no comércio é reduzido não apenas para grandes empresas, mas também para indivíduos, pequenas empresas e empreendedores.

Os efeitos da transformação digital também se manifestam na destruição e criação de empregos em diferentes setores, no surgimento de novas formas de trabalho e em um cenário de remodelação do comércio, principalmente de serviços. Nos países em desenvolvimento, as atividades sociais, econômicas e financeiras online foram facilitadas por meio da adoção de telefones celulares e maior conectividade com a internet.

Na economia da informação, grandes quantidades de informações são coletadas, armazenadas, processadas e transmitidas diariamente em todo o mundo, graças aos avanços na capacidade computacional e comunicacional.

A capacidade de mover dados livremente através das fronteiras sustenta uma crescente gama de atividades econômicas e comércio internacional. O comércio já foi dominado por bens tangíveis e estava em grande parte confinado às economias avançadas e suas grandes empresas multinacionais. Hoje, os fluxos globais de dados estão aumentando e as plataformas digitais permitem a participação de mais países e empresas menores.

Desde o monitoramento de máquinas no chão de fábrica até o acompanhamento do progresso de navios no mar ou de encomendas transportadas através de fronteiras, a coleta, o armazenamento, o processamento e o movimentação de dados estão ajudando as empresas a obterem melhores resultados.

No entanto, ao mesmo tempo em que gera novos modelos de negócios e um escopo mais amplo de inovação, os fluxos internacionais de dados internacionais também levantam preocupações.

O fornecimento online de serviços de pesquisa, comunicação, saúde, educação, varejo e financeiro depende ou pode levar à coleta de dados pessoais. A natureza global da Internet significa que esses dados podem ser rápida e facilmente transferidos para terceiros em outras jurisdições. Essa transferência pode violar a privacidade quando os dados pessoais são remetidos para países que não oferecem níveis adequados de proteção.

Promover um ambiente online seguro é um desafio fundamental para garantir que as oportunidades emergentes da economia da informação possam ser totalmente aproveitadas. O tratamento de dados é uma variável central dessa equação. No

mundo digital de hoje, os dados pessoais são o combustível que impulsiona muitas atividades econômicas.

A proteção de dados é um campo cada vez mais importante, principalmente devido à expansão da economia digital. À medida que mais modelos e práticas de negócios são realizados através de plataformas digitais e os dados se tornam cada vez mais compartilhados em escala internacional, sua relação com o comércio internacional se intensifica.

Assim, à medida que crescem as atividades econômicas e sociais realizadas no mundo virtual, a importância da proteção dos dados pessoais é cada vez mais reconhecida, principalmente no contexto do comércio internacional.

Essa preocupação tem levado reguladores a proibirem ou limitarem o livre fluxo de dados através das fronteiras, com reflexos sobre o comércio internacional.

Como os dados são coletados, digitalizados, armazenados e movidos em uma base verdadeiramente global por uma infinidade de partes, as restrições às transferências internacionais de dados afetam diretamente o comércio internacional.

O atual ambiente regulatório sobre proteção de dados está longe de ser o ideal. Alguns países não possuem regras vigentes; noutros casos, são previstas diversas exceções e regulamentos são incompatíveis entre si. Essa falta de clareza cria incertezas para consumidores e empresas, limita as possibilidades de trocas comerciais internacionais e impede o crescimento econômico.

Ademais, as regras comerciais multilaterais existentes foram negociadas quando o comércio digital estava em sua infância e, mesmo se originalmente concebidas como tecnologicamente neutras, surgiram questões sobre se elas poderiam exigir modernização para refletir novas formas e problemas do comércio digital.

Assim, os governos serão desafiados a adaptar seus sistemas regulatórios para lidar com esse aumento na digitalização e no comércio digital. Os formuladores de políticas precisarão abordar questões delicadas em torno da segurança dos dados, privacidade e governança da internet.

Compreender diferentes abordagens e possíveis vias para estabelecer estruturas jurídicas mais compatíveis nos níveis nacional, regional e multilateral é importante para facilitar o comércio internacional.

A questão é crítica para o futuro do comércio internacional.

Esse é o contexto que se insere o presente trabalho, que tem como objetivo analisar o regime jurídico internacional da proteção de dados pessoais e seus reflexos no comércio internacional, com ênfase nas transferências internacionais de dados pessoais.

A metodologia empregada na dissertação foi, basicamente, de pesquisa qualitativa de dados secundários nacionais e internacionais (desde livros até artigos de revistas especializadas, incluído nesse rol aqueles disponíveis em meio físico e eletrônico), através do estudo histórico, monográfico e comparativo da doutrina, teorias e legislação atinentes ao tema. Também realizou-se rigorosa pesquisa jurisprudencial no âmbito do Tribunal de Justiça da União Europeia (TJUE), para, a partir da análise dos precedentes disponibilizados no *site* do tribunal, traçar um panorama tendente a conferir maior didática no estudo do tema, bem como almejando a estabelecer certa previsibilidade na análise da matéria.

1. UM MUNDO DE DADOS

1.1. A nova globalização e a digitalização da economia

Por muito tempo, a circulação de bens, serviços e capitais esteve por trás da ideia de globalização, ampliando e aprofundando as conexões entre pessoas, empresas e nações.

Na "globalização do século XX" [1] (MGI, 2016, p. 24), o crescimento e aprofundamento das relações econômicas internacionais estiveram diretamente relacionadas com o comércio de bens e serviços e a circulação internacional de capitas[2].

Entre 1985 e 2007, o comércio mundial de bens cresceu duas vezes mais rápido do que o PIB mundial, decorrência do movimento encabeçado pelas grandes multinacionais de expansão das cadeias de produção e realização de investimentos estrangeiros diretos[3] em economias emergentes, objetivando aproveitamento de mão de obra abundante e barata (não apenas no sentido financeiro, mas também no que se refere a maior flexibilidade de direitos e garantias trabalhistas previstos pela legislação local) disponível (MGI, 2016, p. 24).

---

[1] Tradução livre do original em inglês: Ïn the 20th-century version of globalization (…)".

[2] Embora tenha mantido um crescimento constante ao longo dos anos, o comércio global de serviços representava (e ainda representa) uma parcela menor do PIB mundial. Embora tenha apresentado um crescimento de 1250% entre 1985 e 2014 (de US$ 400 milhões para US$ 5 bilhões), o comércio de serviços contribui com apenas 6,3% do PIB mundial, ainda longe dos US$ 19 trilhões anuais movimentados pelo comércio de bens (MGI, 2016, p. 28).

[3] Sobre o assunto, ver CLOSS (2010), DIAS (2010) e COSTA (2010). Segundo COSTA (2010, p. 37 e 38), "A busca da maior produtividade em relação ao custo – influenciada pelo preço e pelo rendimento de fatores de produção, como mão de obra e recursos naturais – é tradicionalmente apontada como a principal razão para a realização de investimentos no exterior. Esse modelo é conhecido como o de busca de eficiência e pode ser implementado pela integração vertical de atividades no interior de uma mesma empresa. Por outro lado, o investimento estrangeiro também pode ocorrer para obter acesso a mercados, quando a empresa pode experimentar expansão horizontal das cadeias de produção (...). Conforme o chamado *OLI paradigm*, que explica o investimento estrangeiro a partir da presença efetiva de três fatores a propriedade (*ownership*) de vantagens que uma firma pode potencializar em um lugar (*location*) que apresenta vantagens em termos regulatórios e de custos e quando há vantagens em internalizar (*internalization*) custos. Vantagens de propriedade referem-se a qualidades de um produto ou processo, bem como as intangíveis, como tecnologia, reputação da marca e habilidades administrativas. Por sua vez, vantagens locacionais se referem a benefícios obtidos com o deslocamento da produção e da oferta, com a superação de barreiras comerciais, naturais (custos de transporte) ou artificiais (tarifas e cotas) e o menor custo de fatores produtivos. Por fim, a internalização se refere a vantagens do investimento sobre o comércio internacional, segundo Brewer e Young (1998), Brenton, Mauro e Lücke (1999) e Molle (2003)".

Uma outra razão para esse crescimento foi a disparada no preço das *commodities* entre os anos 2000 e 2011, impulsionada pela rápida urbanização e industrialização de economias emergentes, que passaram a demandar cada vez mais matérias-primas, como aço e cobre (MGI, 2016, p. 24).

Atualmente, o cenário é outro. Embora o comércio tradicional de bens tenha se recuperado e experimentado crescimento nos anos seguintes à crise financeira global de 2008, não conseguiu atingir o mesmo patamar das últimas duas décadas do século XX e da primeira década do século XXI (MGI, 2016, p. 24 a 26).

Esse movimento do mercado pode ser explicado por diversos fatores cíclicos, como a desaceleração do crescimento das economias chinesa, europeia e japonesa (MGI, 2016, p. 25), e estruturais, como o aumento do consumo da produção local nos mercados emergentes e o encurtamento das cadeias de produção globais (MGI, 2016, p. 25 e 26).

Nesse contexto, o *McKinsey Global Institute* destaca o impacto que as impressoras 3D podem causar no comércio internacional de bens, especialmente eletrônicos, autopeças, instrumentos médicos e vestuário, uma vez que tais produtos poderão ser “impressos” no local onde serão consumidos (MGI, 2016, p. 26 e 27). A OCDE (2017, p. 204) também ressalta os efeitos negativos da impressão 3D sobre o processo produtivo, uma vez que, devido à rápida criação de protótipos, a tendência é que ocorra um encurtamento das cadeias de valor globais e, por conseguinte, do comércio internacional.

Embora possa representar um aumento na produtividade, pela diminuição no número de intermediários e do desperdício de materiais, não há dúvidas de que uma das consequências imediatas da massificação das impressoras 3D será a redução do comércio internacional, especialmente de insumos e produtos intermediários, a exemplo da Boeing, multinacional norte-americana de desenvolvimento aeroespacial e de defesa, que já utiliza impressão 3D para mais de 20 mil unidades de 300 peças distintas (DAVIDSON, 2012 apud OCDE, 2017, p. 204).

Da mesma forma que o comércio de bens, a circulação de capitais, incluindo empréstimos, investimentos estrangeiros diretos e aquisição de participações societárias e títulos, cresceu mais rápido do que o PIB mundial entre o final dos anos 1980 e a primeira década do século XX (MGI, 2016, p. 27). Desde a crise financeira

global de 2008, no entanto, o cenário é de contração das remessas internacionais de capitais, à exceção daquelas feitas por migrantes para seus países de origem, que têm crescido cerca de 7% ao ano, alcançando a expressiva cifra de US$ 583 bilhões movimentados anualmente (MGI, 2016, p. 28).

Já o comércio de serviços continua a crescer, ainda que num ritmo lento[4]. No entanto, diferentemente do comércio de bens, que tende a ser impactado negativamente pelas novas tecnologias, a tendência é que o comércio de serviços seja impulsionado pela digitalização da economia (processo de *servicificação*), especialmente pela expansão de tecnologias digitais, do acesso à internet[5] e dos *marketplaces online*, que "(...) tornou mais fácil do que nunca a demanda por ofertas em tempo real, tanto local quanto globalmente" (OCDE, 2017, p. 206).

Nesse sentido, segundo o *McKinsey Global Institute*, o comércio de serviços digitais mais do que dobrou entre 2004 e 2014, totalizando US$ 2,4 trilhões, cerca de 50% do total de serviços exportados (MGI, 2016, p. 28). Dados semelhantes também são apontados pela Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD, do inglês *United Nations Conference on Trade and Development*), segundo a qual cerca de 50% do comércio global de serviços já é digitalizado (CASTRO e MCQUINN, 2015, p. 1).

Se a ampliação e o aprofundamento da circulação de bens, serviços e capitais impulsionaram o processo de globalização durante o século XX, especialmente em suas três últimas décadas, a globalização do século XXI é marcada pela ubiquidade e penetração das novas tecnologias, muitas delas potencialmente disruptivas[6-7], e sua intrínseca relação com a economia e a sociedade.

---

[4] Cerca de 8,8% ao ano (MGI, 2016, p. 28).

[5] A importância da internet para o atual momento histórico é destacada por CASTELLS (2016, p. 100): "Cada grande avanço em um campo tecnológico específico amplifica os efeitos das tecnologias da informação conexas. A convergência de todas essas tecnologias eletrônicas no campo da comunicação interativa levou à criação da internet, talvez o mais revolucionário meio tecnológico da Era da Informação".

[6] BURRI (2019, p. 74 e 75) aponta cinco características essenciais das tecnologias disruptivas: **(a)** elas avançam rapidamente; **(b)** possuem amplo potencial de impacto; **(c)** produzem valor econômico significativo; **(d)** seu impacto econômico é potencialmente transformador. Dessa forma, ela considera disruptivas as tecnologias que possuem o potencial de alterar o *status quo*, impactando a maneira como as pessoas vivem e trabalham, reorganizando as estruturas das indústrias e substituindo negócios existentes.

[7] Como exemplo de tecnologias disruptivas, pode-se citar internet das coisas, computação na nuvem, robótica avançada, veículos autônomos, impressoras 3D etc.

Ao reduzir o custo das transações e possibilitar a circulação instantânea de bens digitais, serviços e capitais, a chamada revolução da tecnologia da informação[8], "(...) evento histórico da mesma importância da Revolução Industrial do século XVIII, induzindo um novo padrão de descontinuidade nas bases materiais da economia, sociedade e cultura" (CASTELLS, 2016, p. 88), inaugurou um novo capítulo na história da globalização[9], em que praticamente todo tipo de transação internacional possui um componente digital [10] (MGI, 2016, p. 30). Nas palavras de FREEMAN (apud CASTELLS, 2016, p. 123):

---

[8] Essas revoluções denotam fases evolutivas no tempo, as quais são comumente relacionadas a certas tecnologias, padrões de produção e processos sociais (BURRI, 2019, p. 75). CASTELLS (2016) considera a revolução da tecnologia da informação, também chamada por ele de "revolução digital" ou "revolução computacional", como a terceira revolução industrial, que teria se iniciado na década de 1960, catalisada pelo desenvolvimento de semicondutores, dos computadores e da internet, e que permanece em curso até hoje. Segundo CASTELLS (2016, p. 88), "A tecnologia da informação é para esta revolução o que as novas fontes de energia foram para as revoluções industriais sucessivas, do motor à vapor à eletricidade, aos combustíveis fósseis e até mesmo à energia nuclear, visto que a geração e a distribuição de energia foram o elemento principal na base da sociedade industrial". Diferentemente, para SCHWAB (2017, p. 6-7), já estaríamos vivendo uma quarta revolução industrial, iniciada entre o final do século XX e início do século XXI, e cujo cerne se refere às tecnologias de processamento de informação e comunicação. Embora reconheça a existência de elementos comuns entre a terceira e quarta revoluções industriais, SCHWAB (2017, p. 2-3) considera que as mudanças promovidas pela quarta revolução industrial são diferentes de tudo aquilo já vivido pela raça humana, por três razões distintas. Primeiramente, o autor considera que a quarta revolução industrial possui uma velocidade exponencial quando comparada com o ritmo linear das revoluções anteriores. Para ele, isso é o resultado do mundo multifacetado e profundamente interconectado em que vivemos e do fato de as novas tecnologias gerarem tecnologias cada vez mais novas e eficientes, num processo de retroalimentação cumulativo entre a inovação e o seu uso. A segunda razão é que ela se baseia na revolução digital e na combinação de múltiplas tecnologias que estão levando a mudanças de paradigmas sem precedentes na economia, negócios, sociedade. Por fim, a quarta revolução industrial envolve a transformação de sistemas inteiros, através de países, empresas, indústrias e sociedade como um todo.

[9] De acordo com CASTELLS (2016, p. 87), "O 'gradualismo', escreveu o paleontólogo Stephen J. Gould, 'o conceito de que toda mudança deve ser suave, lenta e firme, nunca foi lido nas rochas. Representava uma tendência cultural comum, em parte uma resposta do liberalismo do século XIX a um mundo em revolução. Porém ele continua a colorir a nossa leitura supostamente objetiva da história da vida... A história da vida, como a vejo, é uma série de situações estáveis, pontuadas em intervalos raros por eventos importantes que ocorrem com grande rapidez e ajudam a estabelecer a próxima era estável'. Meu ponto de partida, e não estou sozinho nessa conjetura, é que no final do século XX vivemos um desses raros intervalos na história. Um intervalo cuja característica é a transformação de nossa 'cultura material' pelos mecanismos de um novo paradigma tecnológico que se organiza em torno da tecnologia da informação. Como tecnologia, entendo, na linha direta com Harvey Brooks e Daniel Bell, 'o uso de conhecimentos científicos para especificar as vias de se fazerem as coisas de uma maneira reproduzível'. Entre as tecnologias da informação, incluo, como todos, o conjunto convergente de tecnologias em microeletrônica, computação (software e hardware), telecomunicações/radiodifusão, e optoeletrônica. Além disso, diferentemente de alguns analistas, também incluo nos domínios da tecnologia da informação a engenharia genética e seu crescente conjunto de desenvolvimentos e aplicações".

[10] A OCDE (2017, p. 24) define "digitalização" como "(...) a conversão de um sinal analógico transmissor de informações (e.g. som, imagem, texto impresso) em bits binários" (Tradução livre do original em

> Um paradigma econômico e tecnológico é um agrupamento de inovações técnicas, organizacionais e administrativas inter-relacionadas cujas vantagens devem ser descobertas não apenas em uma nova gama de produtos e sistemas, mas também e sobretudo na dinâmica da estrutura dos custos relativos de todos os possíveis insumos para a produção. Em cada novo paradigma, um insumo específico ou conjunto de insumos pode ser descrito como o 'fator-chave' desse paradigma caracterizado pela queda dos custos relativos e pela disponibilidade universal. A mudança contemporânea de paradigma pode ser vista como uma transferência de uma tecnologia baseada principalmente em insumos baratos de energia para uma outra que se baseia predominantemente em insumos baratos de informação derivados do avanço da tecnologia em microeletrônica e telecomunicações.

As tecnologias da informação e da comunicação (TIC) potencializam a inovação ao acelerar a difusão de informações, facilitar o relacionamento entre empresas, aproximando-as dos consumidores, reduzir distâncias geográficas e tornar a comunicação mais eficiente (OCDE, 2017, p. 197). Conforme destacado por MITCHELL e MISHRA (2019, p. 2), "[O]s modernos serviços desempenham um importante papel facilitando a atividade das empresas ao longo da cadeia global de valor, especialmente ao permiti-las movimentar dados de forma rápida e eficiente através dos países"[11].

Os avanços em tecnologia, comunicação, ciência, transportes e indústria, incluindo a liberalização do comércio internacional, resultado das rodadas de negociação realizadas ainda durante o Acordo Geral de Tarifas e Comércio (GATT-1947) e que culminaram na fundação da Organização Mundial do Comércio (OMC) (KUNER, 2013, p. 32), têm acelerado o ritmo da integração global.

CASTELLS (2016, p. 124 e 125) aponta cinco características fundamentais desse novo paradigma introduzido pela digitalização da economia, assim considerada a habilidade de expressar informações (áudio, texto, imagens etc) em códigos binários (bits e bytes), cujas principais características são o aumento da velocidade de processamento; o aumento da capacidade de armazenagem; o aumento da velocidade de transmissão; a melhora da capacidade de compressão de softwares; e

---

inglês: "Digitisation is the conversion of an analogue signal conveying information (e.g. sound, image, printed text) to binary bits").

[11] Tradução livre do original em inglês: "Modern-day digital services play an important role in facilitating businesses across the global supply chain, particularly by enabling them to expeditiously and efficiently move data across countries".

a padronização de softwares. Segundo BURRI (2019, p. 78), a digitalização "liberta a informação de um meio tangível, e a torna fácil de se trabalhar em rede"[12].

A primeira característica é que a informação é a principal matéria-prima, isto é, são tecnologias para agir sobre a informação, não apenas informação para agir sobre a tecnologia, como foi o caso das revoluções tecnológicas anteriores.

A segunda característica é a maior ubiquidade e penetrabilidade dos efeitos das novas tecnologias, que estão presentes em cada vez mais aspectos das nossas vidas, influenciando diretamente nossos comportamentos enquanto indivíduos e os rumos da nossa sociedade, tanto em questões econômicas quanto político-sociais. De acordo com CASTELLS (2016, p. 124), "[C]omo a informação é uma parte integral de toda atividade humana, todos os processos de nossa existência individual e coletiva são diretamente moldados (embora, com certeza, não determinados) pelo novo meio tecnológico"[13].

A terceira característica se refere aos sistemas de redes, que possuem estrutura descentralizada, poder computacional distribuído através dos seus "nós" (roteadores e comutadores eletrônicos), funções redundantes para diminuir o risco de desconexão e apresentam crescimento exponencial, ao passo que seus custos crescem linearmente. Segundo CASTELLS (2016, p. 124):

> A morfologia da rede parece estar bem adaptada à crescente complexidade de interação e aos modelos imprevisíveis do desenvolvimento derivado do poder criativo dessa interação. Essa configuração topológica, a rede, agora pode ser implementada materialmente em todos os tipos de processos e organizações graças a recentes tecnologias da informação. Sem ela, tal implementação seria bastante complicada. E essa lógica de redes, contudo, é necessária para estruturar o não estruturado, porém preservando a flexibilidade, pois o não estruturado é a força motriz da inovação na atividade humana.
>
> Ademais, quando as redes se difundem, seu crescimento se torna exponencial, pois as vantagens de estar na rede crescem exponencialmente,

[12] Tradução livre do original em inglês: "(...) it frees information from a tangible medium, and makes it networkable and easy to manipulate".

[13] Ainda sobre a relação entre sociedade e tecnologia, CASTELLS (2016, p. 66) destaca, em outra passagem do livro, que "(...) embora não determina a tecnologia, a sociedade pode sufocar seu desenvolvimento principalmente por intermédio do Estado. Ou então, também principalmente pela intervenção estatal, a sociedade pode entrar num processo acelerado de modernização tecnológica capaz de mudar o destino das economias, do poder militar e do bem-estar social em poucos anos. Sem dúvida, a habilidade ou inabilidade de as sociedades dominarem a tecnologia e, em especial, aquelas tecnologias que são estrategicamente decisivas em cada período histórico, traça seu destino a ponto de podermos dizer que, embora não determine a evolução histórica e a transformação social, a tecnologia (ou sua falta) incorpora a capacidade de transformação das sociedades, bem como os usos que as sociedades, sempre em um processo conflituoso, decidem dar ao seu potencial tecnológico".

> graças ao número maior de conexões, e o custo cresce em padrão linear. Além disso, a penalidade por estar fora da rede aumenta com o crescimento da rede em razão do número em declínio de oportunidades de alcançar outros elementos fora da rede.

Em quarto lugar, o paradigma da tecnologia da informação é baseado na flexibilidade, ou seja, "[N]ão apenas os processos são reversíveis, mas organizações e instituições podem ser modificadas, e até mesmo fundamentalmente alteradas, pela reorganização de seus componentes" (CASTELLS, 2016, p.124).

Por fim, verifica-se o que CASTELLS (2016, p. 125) chama de "convergência de tecnologias específicas para um sistema altamente integrado", no qual não é possível distinguir tecnologias mais antigas isoladamente, mas apenas no contexto em que utilizadas, normalmente associadas a outras tecnologias mais recentes. Nesse sentido, a combinação de tecnologias digitais, possibilitando o desenvolvimento de novas aplicações, é apontada pela OCDE como um dos principais motivos pelos quais tais tecnologias são tão importantes para a transformação do processo produtivo (2017, p. 203-204).

Essa nova era hiperconectada e hiper-rápida dos fluxos globais (MGI, 2016, p. 30), em que economias por todo mundo passam a manter uma relação de interdependência global (CASTELLS, 2016, p. 61), é influenciada por três fenômenos distintos, porém complementares, responsáveis por moldar a nova globalização (MGI, 2016, p. 33).

O primeiro desses fenômenos são as plataformas digitais[14], que ampliam mercados para bens e serviços, físicos e digitais (OCDE, 2017, p. 206), sendo

[14] KHAN (2015, p. 789) considera que "Embora as plataformas formem a espinha dorsal da economia digital, suas implicações para o direito vigente ainda são pouco teorizadas" (Tradução livre do original em inglês: "Although platforms form the backbone of the internet economy, the way that platform economics implicates existing laws is relatively undertheorized"). Plataformas digitais não são meras ferramentas; são verdadeiros modelos de negócios, com poder de influência cada vez maior (*lex mercatória digital*), cujas características (mercados de dois ou mais lados e efeitos de rede) as levam a ser monopólios virtuais. Uma das particularidades dos mercados digitais é o fato deles serem quase sempre mercados de dois (ou mais) lados (*two-sided* ou *multisided platforms*), nos quais os chamados efeitos de rede (diretos e indiretos) têm importância crucial. Efeito de rede é o resultado que a quantidade de usuários tem sobre o valor de um bem ou serviço. Em outras palavras, quando o efeito de rede está presente, o benefício de um produto ou serviço aumenta conforme o número de usuários também aumenta. Plataformas digitais geram um feedback positivo do lado da demanda, pois a utilidade de uma plataforma cresce à medida que aumenta seus números de usuários. Isso pode levar ao fenômeno conhecido como *market tipping*, quando uma plataforma se torna mais relevante do que

apontadas como um dos negócios digitais mais bem-sucedidos dos últimos 15 anos[15] (OCDE, 2017, p. 197).

Com o surgimento e a expansão das plataformas digitais, que incluem *e-commerces* (*Amazon*, *Alibaba*, *eBay*), sistemas operacionais (*Android*, da *Google*; IOS, da *Apple*; *Windows Phone*, da *Microsoft*), redes sociais (*Facebook*, *Instagram*, Twitter, Tinder), plataformas de conteúdo digital (*Spotify*, *Netflix*, *Youtube*), *marketplaces* (*Linkedin*, *Upwork*[16], *Kiva*[17], *Kickstarter*[18], *Khan Academy*[19], *Airbnb*), verificou-se uma redução nos custos relacionados às interações e transações internacionais[20], possibilitando a ampliação da oferta e da demanda, bem como o ingresso de novos participantes no comércio internacional (MGI, 2016, p. 35). Nesse sentido, PORGES e ENDERS (2016, p. 2) observam que:

> Surgiu uma nova ocupação, o comerciante online, concentrando-se em pedidos pequenos, e não nos pedidos em massa que normalmente dominam as cadeias de suprimentos *business-to-business* (B2B). As pequenas e médias empresas (PMEs) produtoras de produtos de nicho podem encontrar uma massa crítica de clientes para seus produtos, serviços ou conteúdo

---

todos seus competidores, naturalmente assumindo uma posição dominante. Entre outras consequências importantes, isso tem implicações concretas e práticas em termos de definição de mercados relevantes e de avaliação de poder de mercado e seu exercício. Além disso, as plataformas digitais apresentam grandes retornos de escala, isto é, o custo de produção é proporcionalmente inferior ao número total de usuários. Outra característica desses mercados é a possibilidade de adoção de certos arranjos contratuais que podem, em tese, desencorajar a entrada de novos players. Tais arranjos podem expulsar ou inibir a entrada de competidores no mercado ao reduzir suas possibilidades de atuação, ou aumentar seus custos, a ponto de tornar-se sua atuação proibitiva. Essas posições privilegiadas podem ser alcançadas por meio de arranjos verticais discriminatórios cujo efeito, ainda que não imediato, poderá ser o de fechamento dos mercados envolvidos. Outro importante aspecto das plataformas digitais está no volume de dados pessoais que elas acumulam de seus usuários. Isto traz discussões sobre privacidade e suas implicações, mas também gera debates sobre uma nova dinâmica competitiva. Num mundo em que a coleta, processamento e utilização de dados cresce exponencial e permanentemente, surgem novas discussões como o uso de dados para discriminação de preços entre usuários ou a relevância de padrões de privacidade como forma de diferenciação não-preço entre as plataformas. A intrínseca relação entre as plataformas digitais e o negócio de dados causa um duplo efeito no plano concorrencial: **(a)** cria uma dinâmica concorrencial própria sobre a utilização e processamento dos dados no seu âmbito, o que impossibilita ou torna consideravelmente difícil a concorrência no mercado de dados fora delas e **(b)** e fomenta uma crescente dependência dos demais agentes econômicos, não rivais, em relação aos seus serviços.

[15] Uma comparação feita pela OCDE (2017, p. 206) mostra que, em 1995, as 15 maiores empresas de tecnologia eram provedores de serviços na internet, mídia digital e fornecedores de software ou hardware, enquanto, em 2017, apenas Apple e Salesforce, empresa americana de software *on demand*, não eram plataformas digitais.

[16] Plataforma global de *freelancing* onde empresas e profissionais independentes se conectam e colaboram remotamente (https://www.upwork.com).

[17] Plataforma que possibilita a obtenção de microcrédito através da internet (https://www.kiva.org).

[18] Plataforma de financiamento coletivo (https://www.kickstarter.com).

[19] Plataforma de educação gratuita (https://pt.khanacademy.org).

[20] Resultado do processo de automatização de processos pelo uso de algoritmos, que reduz os custos marginais das plataformas a praticamente zero (MGI, 2016, p. 34).

> digital online, contando principalmente com mercados, como eBay, Amazon, Etsy ou iTunes[21].

Do ponto de vista da demanda, ao concentrarem milhares de comerciantes num único local, promovendo uma concorrência natural entre eles, as plataformas digitais fornecem uma enorme variedade de produtos a preços competitivos (MGI, 2016, p. 35), sendo a maior transparência na prestação de informação ao consumidor considerada uma das importantes consequências do processo de digitalização da economia:

> Uma importante consequência desses fatores tem sido o crescimento exponencial da oferta de informações disponíveis para o consumidor. Em razão disso, consumidores aprenderam a utilizar ferramentas para buscar e selecionar informações de valor e se tornaram mais sensíveis à reputação e à marca como formas de reconhecerem a relevância e qualidade das informações.[22]

Da mesma forma, para a OCDE (2017, p. 208), os principais benefícios das plataformas digitais, quando comparadas com o comércio tradicional, são a acessibilidade e os preços baixos. Amplia-se, assim, a possibilidade de escolha dos cerca de 360 milhões de pessoas que, a cada ano, participam do comércio eletrônico internacional (MGI, 2016, p. 49), número maior do que toda a população dos Estados Unidos, estimada em 328,7 milhões.

Em razão da diminuição dos custos envolvidos e dos potenciais ganhos econômicos a serem alcançados, as plataformas digitais abriram as portas do comércio internacional para novos participantes, especialmente pequenas e médias empresas (PME's), para passaram a competir diretamente com grandes corporações.

Antes, as empresas tinham que crescer substancialmente para poderem arcar com os custos de exportação, mas a digitalização reduziu as barreiras de entrada do

---

[21] Tradução livre do original em inglês: "A new occupation, the online trader, has emerged, focusing on small orders, rather than the bulk orders that typically dominate business-to-business (B2B) supply chains. Small and medium-sized enterprises (SMEs) producing niche products can find a critical mass of customers for their goods, services, or digital content online, mainly relying on marketplaces, such as eBay, Amazon, Etsy, or iTunes".

[22] Tradução livre do original em inglês: "An important consequence of these factors has been the exponential growth of information offerings available to the consumer. As a result, consumers have learned to reach for tools to screen and select information of value and have become more sensitive to reputation and branding as a way of recognizing relevance and quality information".

mercado internacional, facilitando o surgimento, crescimento e gerenciamento de novos negócios (OCDE, 2017, p. 199).

Isso é especialmente relevante para as PME's, que passam a ter acesso a toda uma infraestrutura (*plug-and-play*) de pagamento, suporte logístico e visibilidade, além de acesso a uma enorme base global de clientes, pois "(...) um site oferece às PME's uma presença internacional instantânea sem a necessidade de estabelecer uma presença física no exterior - geralmente uma opção economicamente inviável para as elas"[23] (MELTZER, 2016, p. 11).

Uma pesquisa realizada pelo eBay em 18 países mostrou que mais de 88% das PMEs que utilizam a plataforma são comerciais-exportadoras (MGI, 2016, p. 23). Para MELTZER (2016, p. 11), as novas tecnologias possibilitaram que as PMEs pudessem se especializar em tarefas específicas e utilizassem a Internet para fornecer serviços ou como parte de uma cadeia de valor global.

As plataformas digitais também facilitam a obtenção de novas fontes financiamento pelas PMEs, um dos principais problemas[24] enfrentados por essas empresas (OCDE, 2017, p. 200). Ao aumentar a transparência e reduzir assimetrias de informação, a internet ajuda na aproximação entre PME's e investidores tradicionais (OCDE, 2017, 201).

Para economias em desenvolvimento, a chegada de novas plataformas digitais têm um impacto maior sobre o comércio de bens e serviços do que em economias avançadas, que já possuem conexões comerciais mais extensas.

De acordo com o MGI (2016, p. 23), países na periferia da rede dos fluxos internacionais de dados se beneficiam mais do que os produtores de conteúdos digitais das economias centrais. Isso porque tais países podem se especializar no que produzem, realizar economias de escala e atrair a concorrência, estimulando a eficiência e a inovação nas indústrias nacionais. De acordo com MELTZER (2016, p. 6):

> A internet também está superando barreiras, o que anteriormente tornava caro para muitas empresas nos países em desenvolvimento o comércio internacional. Por exemplo, a capacidade de fornecer produtos digitais on-line pode ajudar a superar os custos comerciais tradicionais decorrentes de

[23] Tradução livre do original em inglês: "(...) a website gives SMEs an instant international presence without having to establish a physical presence overseas – often not an economic option for SMEs".
[24] O segundo principal obstáculo enfrentado pela PME's, identificado pela OCDE (2017, p. 202), são as questões regulatórias, que tocam às discussões travadas no capítulo 02.

> infraestrutura deficiente, procedimentos aduaneiros ineficientes e distância a grandes mercados consumidores[25].

Do ponto de vista da oferta, as plataformas digitais fornecem aos comerciantes uma enorme base de potenciais consumidores, possibilitando a venda direta e o lançamento de novos produtos (MGI, 2016, p. 35). De acordo com PORGES e ENDERS (2016, p. 2), “Para as empresas, o comércio digital elimina as restrições do mercado doméstico/regional, possibilitando a venda para clientes em todo o mundo ou a obtenção de insumos, produtos ou serviços de uma infinidade de novos fornecedores”[26].

A digitalização também expõe as empresas a uma maior concorrência e às melhores práticas de gestão e governança internacionais, estimulando-as a melhorarem seu desempenho e produtividade. Por exemplo, o uso da internet para coleta e análise de dados pode melhorar a produtividade das empresas ao tornar as cadeias produtivas mais eficientes e melhorar o transporte e a distribuição de mercadorias.

Assim, tais plataformas são responsáveis pela criação de mercados verdadeiramente globais e comunidades de usuários numa escala sem precedentes (MGI, 2016, p. 33), a exemplo do *Facebook*, que, ao completar 15 anos de existência, em fevereiro de 2019, atingiu a impressionante marca de 2,3 bilhões de usuários[27], cerca de 30% da população mundial, estimada em 7,794 bilhões de pessoas, segundo o relatório *Perspectivas Mundiais de População 2019: Destaques*, recentemente publicado pela Divisão de População do Departamento da ONU de Assuntos Econômicos e Sociais. Se o *Facebook* fosse um país, seria o mais populoso do mundo, superando China e Índia, atuais primeira e segunda colocadas, com 1,439 e 1,380 bilhão, respectivamente.

---

[25] Tradução livre do original em inglês: “The internet is also overcoming barriers the previously made it costly for many businesses in developing countries to engage in international trade. For example, the ability to deliver digital products online can help overcome traditional trade costs aris-ing from poor infrastructure, inefficient customs procedures, and distance to large consumer markets”.

[26] Tradução livre do original em inglês: “For business, digitally enabled trade lifts constraints of the domestic/regional market, creating opportunities to sell to costumers all over the world, or source inputs, products, or services from a myriad of new suppliers”.

[27] https://g1.globo.com/economia/tecnologia/noticia/2019/02/04/facebook-completa-15-anos-com-23-bilhoes-de-usuarios.ghtml

Segundo MGI (2016, p. 34), cerca de 16% do comércio eletrônico B2C (*business-to-consumer*) é internacional, e estima-se que essa parcela atinja quase 30% até 2020, quando as transações internacionais alcançarão US$ 1 trilhão. O comércio eletrônico B2B (*business-to-business*) é ainda maior, tendo alcançado, ainda em 2014, a cifra de US$ 2 trilhões. Em 2015, 12% do comércio mundial de bens foi realizado eletronicamente, movimentando cerca de US$ 2,2 trilhões.

A rapidez com que produtos e serviços digitais são comercializados, a baixíssimo custo, é outra marca da nova globalização (MGI, 2016, p. 35-37; OCDE, 2017, p. 203). Livros eletrônicos (e-books), aplicativos para *smartphones* (*app economy*), jogos *online*, serviços de *streaming* (Netflix, Spotify) e *softwares*, por exemplo, podem ser transmitidos virtual e instantaneamente para consumidores em qualquer parte do mundo, bastante apenas uma conexão com a internet.

O terceiro fenômeno resultante da digitalização é a adição de componentes digitais a bens e serviços tradicionais, promovendo o desenvolvimento de novas aplicações para esses produtos (OCDE, 2017, p. 203 e 204) e, por conseguinte, a geração de maior valor agregado (MGI, 2016, p. 37).

À medida que os bens se tornaram *commodities* com baixa margem de lucro, muitas indústrias passaram a desenvolver serviços complementares às suas atividades tradicionais (OCDE, 2017, p. 203). Por exemplo, ao se tornarem *data* intensivos, tratores deixam de ser um mero produto físico, para se transformarem em um dos vários componentes de um pacote de serviços mais abrangente, que inclui monitoramento e cultivo do solo, com o envio de dados aos proprietários através de aplicativos (OCDE, 2017, p. 196). Isso possibilita a tomada de decisões em tempo real, evitando desperdícios e aumentando a produtividade e a qualidade dos produtos e, por conseguinte, a competitividade em escala global.

Além desses fatores, AHMED e ALDONAS (2015, p. 1) apontam ainda o ritmo acelerado de inovação em tecnologias da informação e comunicação; a redução no preço de *smartphones* e *tablets*; e o maior acesso à internet de banda larga. Para eles, a cobertura de rede mais ampla, a expansão da capacidade de transferência de dados, e a facilitação do acesso a equipamentos eletrônicos e conexões de banda larga possibilitaram a criação de novos modelos de negócios. Nesse mesmo sentido, MELTZER (2016, p. 9) afirma que:

> Também é o caso de que o acesso à Internet está cada vez mais acontecendo em dispositivos móveis, tornando o acesso a esses dispositivos inseparáveis do desafio de expandir o acesso à Internet. De fato, os telefones celulares são agora a principal maneira de as pessoas nos países em desenvolvimento ficarem online. Os desafios para expandir esse acesso à Internet incluem os custos de smartphones habilitados para a Internet e os custos dos planos de banda larga móvel[28].

Por fim, ao criar postos de trabalho em áreas como TIC, serviços e *software*, a internet também beneficia a empregabilidade. A USITC descobriu que a internet está diretamente relacionada com o aumento dos empregos nos EUA em cerca de 1,8% (USITC, 2014, p. 71). Um relatório da MGI (2011) constatou que, para cada empregado que deixou de existir por conta da internet, são criadas 2,6 novas ocupações.

A evolução dos chamados empregos contingentes (*freelancers*), possibilitada pela transformação digital, não está apenas mudando a natureza dos arranjos de trabalho, oferecendo oportunidades de emprego flexíveis, mas também criando uma lacuna no acesso a benefícios sociais.

Essas mudanças são ainda maiores e mais complexas na medida em que estão ocorrendo ao mesmo tempo e em países com diferentes custos de fatores de produção, níveis de desenvolvimento econômico, social e tecnológico e regimes regulatórios.

1.2. Economia de dados

A globalização e a digitalização da economia alcançaram um nível tal que não nos parece absurda a afirmação de que o mundo se encontra atualmente numa “era digital” (CASALINI e GONZÁLEZ, 2019, p. 8), em que comércio e produção dependem, cada vez mais, da capacidade de armazenamento, utilização e transferência de dados, informações e conhecimentos.

---

[28] Tradução livre do original em inglês: “Its also the case that internet access is increasingly happening over mobiles devices, making access to such devices in-separable form the challenge of expanding internet access. Indeed, mobile phones are now the main way that people in developing countries get online. Challenges to expanding such Internet access include the costs of Internet-enabled smartphones and the costs of mobile broadband plans”.

Em razão das novas tecnologias e de sua profunda integração com todos os aspectos da vida em sociedade, empresas tem capturado grandes volumes de informações sobre seus consumidores e fornecedores e sobre sua própria operação.

Nessa nova era, embora uma importante parcela da economia mundial ainda corresponda à circulação de bens, serviços e capitais, a globalização está sendo acelerada e redefinida pela circulação de dados. Segundo dados da OCDE (2017, p. 202), a cada semana, produz-se mais dados do que em todo último milênio; diariamente, o volume de dados movimentados equivale à capacidade de armazenamento necessária para gravar 50 mil anos em DVD's.

A utilização de dados promete aperfeiçoar produtos, processos, métodos organizacionais e mercados (OCDE, 2017, p. 202). Na agricultura, mapas geocodificados das lavouras e monitoramento em tempo real de todas as atividades agrícolas, desde a plantação até a colheita, incluindo padrões climáticos, condições do solo, uso de fertilizantes, são utilizados para aumentar a produtividade e a qualidade dos produtos (OCDE, 2017, p. 202 e 203). Na indústria, dados obtidos através de sensores são utilizados para monitorar e analisar a eficiência de máquinas com o objetivo de otimizar suas operações e oferecer serviços pós-venda, incluindo manutenção preventiva (OCDE, 2017, p. 202). Para BURRI (2019, p. 81):

> O potencial transformador é enorme e se refere não apenas às novas áreas da tecnologia, como pesquisa e redes sociais, mas também para negócios tradicionais. Os dados coletados durante na manufatura, por exemplo, por ajudar a aprimorar processos, antecipar riscos, e prevenir acidentes; a administração do setor público também pode ser mais bem estruturada, tornada mais eficiente e orientada ao cidadão[29].

Embora ainda haja poucas evidências macroeconômicas sobre o impacto da utilização de dados nos modelos de negócios e no mercado (OCDE, 2017, p. 202), estudos sugerem um aumento na produtividade nas empresas. Utilizando o valor dos fluxos para cada país normalizado pelo seu tamanho, entre 2006 e 2016, todos os tipos de fluxos juntos (dados, bens, serviços, capital, pessoas) elevaram o PIB mundial

[29] Tradução livre do original em inglês: "The transformative potential is great and refers not only to new digital native areas, such as search or social networking, but also to brick-and-mortar, physical businesses. The data gathered in manufacturing, for instance, can help improve processes, anticipate risks, and prevent accidents; public sector administration can also be better structured, made more efficient, and more citizen-oriented".

em 10,1% em comparação ao resultado sem nenhum fluxo internacional. Num segundo modelo econométrico, formulado com base no Índice de Conectividade MGI, esse percentual chega a 18,7%, o equivalente a US$ 14,4 trilhões (MGI, 2016, p. 76-77).

Tradicionalmente, a transformação digital dos modelos de negócios foi possibilitada pela formalização e codificação das atividades empresariais, o que levou à automação dos processos através da utilização de softwares (OCDE, 2017, p. 203).

Hoje os modelos de negócios digitais mais bem-sucedidos vão além da formalização e codificação de processos produtivos através de *softwares*. Pela coleta e análise de um enorme volume de dados, muitos dos quais são fornecidos pelos próprios consumidores, e da associação de tais dados com inteligências artificiais, empresas são capazes de automatizar seus processos produtivos e testar e desenvolver novos produtos (bens e serviços) e modelos de negócio mais rapidamente do que a indústria tradicional (OCDE, 2017, p. 203).

A análise desses novos modelos de negócios digitais permite identificar as medidas frequentemente adotadas por essas empresas, como a digitalização de ativos físicos, desde os (já ultrapassados) CD's e DVD's até os modernos escâneres e impressoras 3D; a interconexão de objetos físicos através da internet das coisas (IoT, do inglês *Internet of Things*), que possibilita a inovação de produtos e processos, a exemplo da Scania AB, empresa sueca fabricante de caminhões, ônibus, e motores a diesel, que gera 17% da sua receita através de novos serviços habilitados pela comunicação sem fio incorporada aos veículos; e a codificação e automação de processos através de *softwares* e inteligência artificial, cuja tecnologia pode ser comercializada para terceiros, como o Gmail, que originalmente funcionava como o e-mail corporativo interno da Google até ser transformado num produto específico (OECD, 2017, p. 204 e 205).

Embora essas medidas dependam da coleta, armazenamento e análise de dados, há outras que apostam no uso de *big data* como elemento central do negócio, como a quantificação de dados relativos ao processo produtivo, isto é, a geração constante de novos dados, não apenas pela digitalização de conteúdo, mas principalmente pelo monitoramento de atividades; a comercialização de dados, uma vez que os dados gerados por um determinado negócio podem ser importantes para

outros mercados, dada a sua natureza não-rival[30]; e a reutilização de dados entre setores da economia, através da integração de informações por toda a cadeia de produção, possibilitando o monitoramento e análise da eficiência de produtos, a otimização de operações por todo o sistema e o oferecimento de serviços pós-venda (OCDE, 2017, p. 205 e 206).

A difusão do acesso à internet e a disseminação de tecnologias digitais permitem que dados e informações sejam transferidos globalmente em tempo real, e essa capacidade está transformando o comércio internacional.

Daí porque o livre fluxo de dados, inclusive através das fronteiras nacionais, é um elemento central do que faz da internet a força poderosa para a transmissão de informação e conhecimento e para o desenvolvimento econômico, especialmente porque empresas podem utilizar a internet para exportar bens; serviços podem ser contratados e consumidos online; a coleta e a análise de dados permitem que novos serviços agreguem valor às exportações de mercadorias; os fluxos globais de dados sustentam as cadeias de valor globais, criando novas oportunidades de negócios; aumenta-se a concorrência internacional e criam-se novos mercados consumidores.

De acordo com CORY (2017, p. 1), a maior digitalização das organizações, associada à utilização de novas tecnologias como *cloud computing* e *data analytics*, aumentou a importância dos dados para o comércio de bens e serviços, impactando não apenas a indústria da tecnologia da informação e comunicação, como também as indústrias tradicionais.

Isso porque as empresas, inclusive as indústrias tradicionais, dependem cada vez mais de dados para diversas finalidades, seja para monitorar sistemas de produção, gerenciar forças de trabalho, coordenar cadeias produtivas, oferecer suporte a produtos e serviços em tempo real ou conhecer melhor o perfil de clientes e fornecedores.

---

[30] Em Economia, rivalidade é a situação em que o consumo de um bem por uma pessoa reduz a quantidade disponível desse mesmo bem para o restante da sociedade. Assim, os dados são não-rivais porque quando uma pessoa os utiliza, não impede outros de os utilizarem também. Sobre a natureza não-rival dos dados, a OCDE (2012, p. 205) esclarece o seguinte: “Além disso, as empresas podem se aproveitar da natureza não-rival dos dados para criarem mercados de múltiplos lados (dentro de uma organização), onde as atividades de um lado do mercados andam de mãos dadas com a coleta de dados, que é explorado e reutilizado no outro lado do mercado (Tradução livre do original em inglês: “In addition, businesses can take advantage of the non-rivalrous nature of data to create multi-sided markets (inside an organisation), where activities on one side of the market go hand-in-hand with the collection of data, which is exploited and reused on the other side of the market”).

Nesse mesmo sentido, CASTRO e MCQUINN (2015, p. 16), ao analisarem os impactos negativos da imposição de limitações às transferências internacionais de dados nas indústrias tradicionais (mineração, manufatura, óleo e gás, varejo, sistema bancário, aeronáutica, saúde, automobilística), concluíram que "em nosso mundo cada vez mais conectado, o acesso à informação está se tornando cada vez mais importante, não apenas para negócios puramente digitais, mas também para companhias tradicionais".

Segundo MELTZER (2015, p. 92), os fluxos globais de dados possibilitam às empresas relacionarem-se com seus clientes em tempo real, adaptando a produção em resposta às preferências dos consumidores, e fragmentarem o processo produtivo em cadeias de valor globais, transferindo as várias etapas do processo produtivo para locais com vantagens comparativas decorrentes de sua localização, beneficiando-se, assim, de menores custos de transação.

Da mesma forma que outros fatores de produção, como recursos naturais e capital humano, a utilização de dados está se tornando imprescindível para o crescimento econômico e inovação.

À medida que os dados se tornam cada vez mais importantes para o desenvolvimento das atividades econômicas, inclusive do comércio internacional, ao ponto de serem considerados "o novo petróleo da era digital"[31-32] (THE ECONOMIST, 2017), "a força vital do comércio na era digital"[33] (CASALINI e GONZÁLEZ, 2019, p. 14), "a força vital da moderna economia global"[34] (CORY, 2017, p. 01), "o novo lubrificante das engrenagens do mercado"[35] (MAYER-SCHÖNBERGER e RAMGE,

[31] Tradução livre do original em inglês: "A new commodity spawns a lucrative, fast-growing industry, prompting antitrust regulators to step in to restrain those who control its flow. A century ago, the resource in question was oil. Now similar concerns are being raised by the giants that deal in data, the oil of the digital era".
[32] Embora a associação entre dados e petróleo seja bastante comum, MANDEL (2017) apresenta uma crítica interessante. Para ele, essa caracterização é equivocada, pois, apesar de os dados serem insumos essenciais para a economia, assim como o petróleo, diferem dele por não serem escassos e poderem ser consumidos por várias pessoas, em razão da sua capacidade de serem copiados e transferidos a um custo relativamente baixo.
[33] Tradução livre do original em inglês: "As data becomes the lifeblood of trade in the digital era, measures that affect its flow are likely to have trade consequences".
[34] Tradução livre do original em inglês: "Data is the lifeblood of the modern global economy".
[35] Tradução livre do original em inglês: "Data is the new grease for the wheels of the market".

2018, p. 63), "a matéria-prima da era da informação"[36-37] (ROSS, 2016, p. 152), devendo, por essa razão, ser incluídos como um quinto item na tradicional lista de questões endereçadas por políticas comerciais (movimento de bens, pessoas, serviços, capital e dados) (CIUARIAK e PTASKHINA, 2018, p. 1), torna-se fundamental entender o que são dados e como ocorre o seu fluxo através da internet.

O debate atual sobre dados e comércio internacional se concentra, basicamente, no fluxo de três diferentes tipos de dados: dados pessoais, dados setoriais (negócios, finanças, saúde etc) e os chamados "dados importantes" (CASALINI e GONZÁLEZ, 2019, p. 11 e 12). De modo semelhante, SEN (2018, p. 21 e 22) classifica os dados em pessoais, da companhia[38], empresariais[39] e sociais[40].

[36] Tradução livre do original em inglês: "Land was the raw material of the agricultural age. Iron was the raw material pf the industrial age. Data is the raw material of the information age".

[37] Nesse sentido, Ginni Rometty, CEO da IBM, no Informe aos Investidores de 2013 (ano em que o número de dados produzidos diariamente no mundo alcançou a incrível marca de 2,5 bilhões de gigabytes), afirmou que "Hoje, toda discussão sobre mudanças em tecnologia, negócios e sociedade deve começar com dados. Em seu volume, velocidade e variedade exponencialmente crescentes, os dados estão se tornando um novo recurso natural. Promete ser para o século XXI o que a energia a vapor foi para o século XVIII, o que a eletricidade foi para o século e o que os hidrocarbonetos foram para o século XX. É isso o que queremos dizer por empresas, instituições e nosso planeta tornando-se mais inteligentes" (Tradução livre do original em inglês: "Today, every discussion about changes in technology, business and society must begin with data. In its exponentially increasing volume, velocity and variety, data is becoming a new natural resource. It promises to be for the 21st century what steam power was for the 18th, electricity for the 19th and hydrocarbons for the 20th. This is what we mean by enterprises, institutions and our planet becoming smarter"). Embora não defina o que entende por informação e conhecimento, nem associe esses conceitos à ideia de "dado" enquanto origem de qualquer informação ou conhecimento, como se verá mais adiante, é possível identificar o mesmo raciocínio em CASTELLS (2016, p. 88): "(...) o cerne da transformação que estamos vivendo na revolução atual refere-se às tecnologias de processamento de informação e comunicação. A tecnologia da informação é para esta revolução o que as novas fontes de energia foram para as revoluções industriais sucessivas, do motor a vapor à eletricidade, aos combustíveis fósseis e até mesmo à energia nuclear, visto que a geração e a distribuição de energia foram o elemento principal na base da sociedade industrial". Em *A Galáxia da Internet: reflexões sobre a internet, os negócios e a sociedade*, CASTELLS (2003, n. p.) defende posição semelhante: "A Internet é o tecido de nossas vidas. Se a tecnologia da informação é hoje o que a eletricidade foi na Era Industrial, em nossa época a Internet poderia ser equiparada tanto a uma rede elétrica quanto ao motor elétrico, em razão de sua capacidade de distribuir a força da informação por todo o domínio da atividade humana. Ademais, à medida que novas tecnologias de geração e distribuição de energia tornaram possível a fábrica e a grande corporação como os fundamentos organizacionais da sociedade industrial, a Internet passou a ser a base tecnológica para a forma organizacional da Era da Informação: a rede".

[38] Dados "da companhia" são aqueles relacionados às atividades operacionais empresas. Tais dados não são monetizados.

[39] Os dados empresariais são aqueles relativos ao comércio, mercados ou que possam ser monetizados.

[40] Dados sociais se referem a padrões de comportamento social.

Para os fins do presente trabalho, considera-se dado pessoal tal qual definido pelas principais normativas nacionais, regionais e internacionais sobre proteção e transferência internacional de dados pessoais.

A *OECD Privacy Guidelines* (OCDE, 2013) define dado pessoal como "qualquer informação relativa a um indivíduo identificado ou identificável"[41]. A Convenção 108 considera dado pessoal "qualquer informação relativa a uma pessoa identificada ou identificável"[42]. A *APEC Privacy Framework* (APEC, 2015, p. 5) utiliza a expressão "informação pessoal", assim considerada "qualquer informação sobre um indivíduo identificado ou identificável"[43]. O Regulamento (EU) 2016/679 da União Europeia[44], denominado Regulamento Geral sobre a Proteção de Dados (GDPR, do inglês *General Data Protection Regulation*), define dado pessoal como a "informação relativa a uma pessoa singular identificada ou identificável" (Artigo 4º (1). No Brasil[45], a Lei n° 13.709/2018[46], denominada[47] Lei Geral de Proteção de Dados Pessoais (LGPD), considera dado pessoal a "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I).

Tais informações devem ser consideradas de forma ampla, ou seja, são consideradas dados pessoais quaisquer informações que possam identificar uma pessoa natural, podendo ser um nome, um número de identificação, elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social, dados de localização, identificadores por via eletrônica, aplicações,

---

[41] Tradução livre do original em inglês: "any information relating to and identified or identifiable individual".
[42] Tradução livre do original em inglês: "'personal data' means any information relating to an identified or identifiable individual".
[43] Tradução livre do original em inglês: "any information about and identified or identifiable individual".
[44] A GDPR entrou em vigor em 25/05/2018, substituindo a legislação anterior sobre proteção de dados pessoais, a Diretiva 95/46//CE.
[45] Até a publicação da LGPD, o Brasil era o único país do Mercosul sem um marco legal da proteção de dados pessoais. Argentina (Ley 25.326), Paraguai (Ley 1682/2001) e Uruguai (Ley 18331) possuem legislações recentes em matéria de proteção de dados. No restante da América do Sul, apenas Equador (com projeto de lei em tramitação), Venezuela, Guiana e Suriname não possuem uma lei geral de proteção de dados.
[46] Publicada desde 15/08/2018, a LGPD entraria em vigor em janeiro/2020, mas o prazo vou adiado agosto/2020. No entanto, já há projeto de lei (PL n° 5.762/2019, proposto pelo deputado federal Carlos Bezerra, do MBD-MT) que pretende adiar o início da vigência da lei por mais dois anos, para agosto/2022.
[47] A ementa original da Lei n° 13.709/2018 era a seguinte: "Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Com a edição da Lei n° 13.853/2019, passou a ser simplesmente "Lei Geral de Proteção de Dados Pessoais (LGPD)".

ferramentas e protocolos, a exemplo dos endereços IP (protocolo internet)[48] ou testemunhos de conexão (*cookies*)[49]. Estes identificadores podem deixar vestígios que, uma vez combinados com outras informações recebidas pelos servidores, podem ser utilizados para a definição de perfis e a identificação de pessoas naturais. Também devem ser consideradas dados pessoais mesmo as informações que, isoladamente, não seriam qualificadas como tal, mas que, em conjunto com outras informações, possibilitam a identificação de uma pessoa natural, a exemplo de certos tipos de metadados, que podem revelar comportamentos individuais, relacionamentos sociais, preferências e, por conseguinte, a identidade de um indivíduo.

Essa acepção amplíssima de dados pessoais também pode ser extraída da jurisprudência do Tribunal de Justiça da União Europeia (TJUE), que em duas oportunidades foi instado a se manifestar sobre o alcance do conceito de dado pessoal"[50-51].

No Acórdão de 19 de outubro de 2016 (C-582/14, EU:C:2016:779), o TJUE analisou questionamento feito pelo Tribunal Federal de Justiça da Alemanha para saber se um endereço de IP registrado por um prestador de serviços quando um indivíduo acessa o seu site constitui um dado pessoal.

No caso, um cidadão alemão requereu judicialmente que a Alemanha fosse proibida de conservar ou mandar conservar por terceiros dados informáticos transmitidos após a consulta de sites dos serviços federais alemães. Com o objetivo de se proteger de ataques e de permitir ações penais contra *hackers*, o prestador de serviços gravava o endereço IP dinâmico[52], a data e a hora dos acessos aos sites.

---

[48] Endereço de Protocolo da Internet (endereço IP) é um número atribuído a cada dispositivo conectado a uma rede de computadores. Um endereço IP serve a duas funções principais: identificação de interface de hospedeiro ou de rede e endereçamento de localização.

[49] Um *cookie* é um arquivo de computador ou pacote de dados enviados por um site para o navegador do usuário, quando ele visita o site. Cada vez que o usuário visita o site novamente, o navegador envia o *cookie* de volta para o servidor para notificar atividades prévias do usuário.

[50] Nos dois casos, a atuação do TJUE se deu em processos de interpretação de legislação (decisões prejudiciais). Se uma jurisdição tem dúvidas sobre a interpretação ou a validade de um ato legislativo europeu, pode pedir esclarecimentos ao TJUE. Esse mecanismo também pode ser utilizado para determinar se uma determinada lei ou prática nacional é compatível com o Direito Europeu.

[51] Embora o TJUE tenha analisado o alcance do conceito de "dados pessoais" à luz da Diretiva 95/46/CE, legislação sobre proteção de dados pessoais vigente à época dos julgamentos (a Diretiva foi recentemente revogada pela Resolução (EU) 2016/679, que passou a disciplinar a matéria), a definição utilizada pelas duas normas é a mesma ("qualquer informação relativa a uma pessoa singular identificada ou identificável"), de modo que as conclusões a que chegou o TJUE continuam válidas.

[52] Um endereço IP "dinâmico" é aquele que muda por ocasião de cada nova ligação à internet.

Diferentemente dos endereços IP estáticos, os endereços IP dinâmicos não permitem, *a priori*, relacionar determinado computador à rede utilizada pelo fornecedor de acesso à internet. Assim, os dados registados, isoladamente, não possibilitariam ao prestador de serviços identificar os usuários. Por outro lado, o provedor de acesso à internet dispunha de informações suplementares que, se combinadas com o endereço IP dinâmico, permitiriam identificar os usuários.

Ao analisar o caso, o TJUE considerou, inicialmente, que, para que um dado qualquer possa ser qualificado como dado pessoal, não é preciso que todas as informações necessárias à identificação de uma pessoa natural estejam na posse de uma única pessoa, seja natural ou jurídica. Assim, o TJUE considerou, ainda, que um IP dinâmico, registrado por um prestador de serviços no momento da consulta ao seu site, constitui um dado pessoal, quando ele disponha de meios legais que lhe permitam identificar a pessoa natural graças às informações suplementares de que o provedor de acesso à internet dispõe.

Já no Acórdão de 20 de dezembro de 2017 (C-434/16, ECLI:EU:C:2017:582), o TJUE analisou questionamento da Suprema Corte da Irlanda para saber se as respostas escritas dadas por um candidato durante um exame profissional e as eventuais anotações do examinador sobre elas constituem dados pessoais.

A ação foi ajuizada por um contabilista irlandês que, após reprovação no exame organizado pela Câmara dos Técnicos Oficiais de Contas, com fundamento no artigo 4º da Diretiva 95/46/CE, teve seu pedido de acesso a todos os dados pessoais que lhe diziam respeito apenas parcialmente atendido pela instituição, que se negou a apresentar-lhe cópia do exame por considerar que tal documento não continha dados pessoais relativos ao candidato. Após sucessivas negativas do Comissário de Proteção de Dados[53] e das instâncias ordinárias do poder judiciário nacional, a matéria chegou à Suprema Corte, que submeteu questão prejudicial à análise do TJUE.

[53] A Diretiva 95/46/CE exigia que cada país membro da União Europeia tivesse uma agência ou comissário de proteção de dados, este último um agente estatal responsável pela supervisão e aplicação dos princípios e leis de proteção à privacidade individual. Atualmente, a GDPR prevê (Capítulo IV, artigos 51° ao 58º) a criação das chamadas Autoridades de Controle Independente, uma ou mais autoridades públicas independentes responsáveis pela fiscalização da aplicação da GDPR, a fim de defender os direitos e liberdades fundamentais das pessoas naturais relativamente ao tratamento e facilitar a livre circulação dos dados pessoais na União Europeia.

Assim como no Acórdão de 19 de outubro de 2016 (C-582/14, EU:C:2016:779), o TJUE reafirmou seu entendimento de que, para que um dado qualquer possa ser qualificado como dado pessoal, não é necessário que todas as informações que permitam identificar uma pessoa natural estejam na posse de uma única pessoa, natural ou jurídica. No caso sob análise, o TJUE entendeu que, ainda que o examinador não tivesse informações suficientes para identificar o candidato no momento da correção do exame, tais informações encontravam-se na posse da Câmara dos Técnicos Oficiais de Contas, possibilitando, assim, a identificação do candidato a partir do seu número de identificação inscrito na capa e na folha de respostas do exame.

Com base nessa premissa, o TJUE concluiu que o conteúdo das respostas escritas fornecidas pelo candidato reflete o seu nível de conhecimento e competência sobre determinada matéria, bem como seu processo de reflexão, julgamento e espírito crítico, constituindo, por essa razão, informações relacionadas à pessoa natural. O TJUE entendeu, ainda, que a utilização dessas informações, que se traduz pela aprovação ou não do candidato, é suscetível de ter efeitos sobre os seus direitos e interesses, na medida em pode determinar ou influenciar as possibilidades de esse candidato aceder profissionalmente.

Em relação às anotações do examinador sobre as respostas do candidato, o TJUE entendeu que elas também constituem informações sobre o candidato, uma vez que refletem a opinião ou apreciação do examinador quantos aos conhecimentos e competências do candidato.

Assim, o TJUE concluiu que as respostas escritas fornecidas por um candidato num exame profissional e as correlatas anotações do examinador constituem dados pessoais, na acepção da legislação europeia sobre proteção de dados pessoais.

Embora as definições vistas acima tomem as expressões “dado”, “informação” e “conhecimento” como sinônimas, a literatura aponta diferenças entre elas (CASALINI e GONZÁLEZ, 2019, p. 11). Os dados se apresentam de forma desordenada ou não processada; uma vez analisados e identificadas possíveis relações entre eles, tem-se uma informação; o conhecimento surge a partir da análise

que reconhece a importância da informação; por fim, sabedoria é fruto de decisões que utilizam o maior fluxo de dados analisados possível.

Nessa chamada hierarquia DIKW (*data-information-knowlegde-wisdom*), cada estágio depende daquele imediatamente anterior. Ao analisar a revolução causada pela tecnologia da informação, CASTELLS (2016, p. 88) aponta que a principal característica dessa revolução é, justamente, "(...) a aplicação desses conhecimentos e dessa informação para a geração de conhecimentos e de dispositivos de processamento/comunicação da informação, em um ciclo de retroalimentação cumulativo entre a inovação e seu uso"[54].

Essa é a razão pela qual comumente se afirma que os dados não possuem um valor intrínseco (CASALINI e GONZÁLEZ, 2019, p. 11) ou que é difícil antecipar o valor que eles agregarão a terceiros (OCDE, 2017, p. 205), de modo que o maior ou menor valor de um dado está diretamente relacionado com a forma como tal dado é utilizado ou aplicado.

A despeito disso, assim como os conceitos e definições estabelecidos pela legislação nacional e estrangeira e pela jurisprudência do TJUE, a presente dissertação utilizará as expressões "dado", "informação" e "conhecimento" indistintamente, partindo da premissa de que a informação e o conhecimento têm origem, necessariamente, nos dados que lhes dão substrato.

Por fim, embora a APEC utilize o termo "informação pessoal", como visto acima, e CASALINI e GONZÁLEZ (2019, p. 12) sugiram a utilização da expressão "informação pessoalmente identificável" como sinônima de dado pessoal, optou-se por utilizar, na presente dissertação, apenas a última expressão, devendo a palavra "dado(s)", doravante, ser compreendida como se referindo, exclusivamente, a "dados pessoais".

A maior penetração da internet e a disseminação e popularização de novas tecnologias possibilitam a movimentação instantânea de dados, transformando, por

[54] Em outras passagens, CASTELLS (2016, p. 90 e 119) reafirma a ideia de que "(...) as novas tecnologias da informação difundiram-se pelo globo com a velocidade da luz em menos de duas décadas, entre meados dos anos 1970 e 1990, por meio de uma lógica que, a meu ver, é característica dessa revolução tecnológica: a aplicação imediata no próprio desenvolvimento da tecnologia gerada, conectando o mundo através da tecnologia da informação" e "(...) o desenvolvimento da revolução da tecnologia da informação contribuiu para a formação dos meios de inovação em que as descobertas e as aplicações interagiam e eram testadas em um repetido processo de tentativa e erro: aprendia fazendo-se".

conseguinte, todos os demais fluxos globais. Nesse contexto, é fora de dúvidas que o comércio internacional depende da coleta, armazenagem, processamento e movimentação de dados pessoais.

1.3. Transformação digital do comércio

O desenvolvimento do comércio internacional também acompanhou e foi diretamente influenciado pelas mudanças de paradigmas sociais, econômicos e tecnológicos ocorridas durante as revoluções industriais[55], especialmente aquelas relacionadas aos modos de produção e aos meios de comunicação e de transporte. Nesse sentido, GONZÁLEZ e JOUNJEAN (2017) apontam a existência de três diferentes estágios de evolução do comércio internacional.

O primeiro, denominado de comércio tradicional, é caracterizado pelo início da segregação da produção e do consumo através das fronteiras nacionais, resultado da queda nos custos dos transportes. Segundo os autores, "Consumidores se beneficiaram do acesso a mais amplo a produtos estrangeiros com preços mais competitivos e o comércio envolveu principalmente produtos finais".

O segundo estágio é o das cadeias globais de valor. Nessa etapa, de acordo com BALDWIN (2016), "O comércio de serviços e produtos intermediários floresceu e a produção global foi realocada, em parte, para economias emergentes". Nesse processo, ocorre a fragmentação do processo produtivo e a transferência de suas várias etapas para locais com vantagens comparativas decorrentes de sua

[55] A palavra "revolução" denota uma mudança abrupta e radical. Ao logo da história, revoluções estiveram diretamente relacionadas ao surgimento de novas tecnologias e formas de perceber o mundo, com profundas mudanças no sistema econômico e estrutura social. A primeira revolução industrial, ocorrida entre os séculos XVIII e XIX, foi possível graças ao surgimento de tecnologias como a máquina à vapor, a fiadeira, o processo Cort em metalurgia e, de modo geral, pela substituição das ferramentas manuais pelas máquinas, inaugurando a produção mecânica. A segunda revolução industrial, iniciada no final do século XIX e que durou até meados do século XX, tornou possível a produção em massa (introdução do conceito de linha de produção), graças ao desenvolvimento da eletricidade, do motor à combustão interna, de produtos químicos, da fundição eficiente do aço e pelo início das tecnologias de comunicação, com a difusão do telégrafo e a invenção do telefone. Ao comentar a primeira e segunda revoluções industriais, CASTELLS (2016, p. 91) afirma que: "Foram, de fato, 'revoluções, no sentido de que um grande aumento repentino e inesperado de aplicações tecnológicas transformou os processos de produção e distribuição, criou uma enxurrada de novos produtos e mudou de maneira decisiva a localização das riquezas e do poder no mundo, que, de repente, ficaram ao alcance dos países e elites capazes de comandar o novo sistema tecnológico". A terceira e quarta revoluções industriais dizem respeito ao surgimento e desenvolvimento das tecnologias da informação e comunicação, vide n. 8.

localização. Com isso, as empresas se beneficiam de menores custos de produção e transação.

O terceiro (a atual) estágio é o do comércio eletrônico ou digital, expressões aqui consideradas como sinônimas, impulsionado pela digitalização da economia e pela redução de custos relacionados à transferência de informações e difusão do conhecimento em escala global. De acordo com GONZÁLEZ e JOUNJEAN (2017, p. 7):

> A digitalização mudou não apenas a maneira como negociamos, mas também o que comercializamos: um número maior de mercadorias pequenas e de baixo valor agregado, além de serviços digitais, agora estão atravessando fronteiras; bens estão cada vez mais integrados a serviços; e novos serviços, anteriormente não negociáveis, estão sendo comercializados internacionalmente. Nesse contexto, a negociação de acesso a mercados e medidas além da fronteira continuam sendo prioridades da política comercial; o comércio digital ainda envolve bens e serviços atravessando fronteiras e aplicações de diferentes regulamentações nacionais. Mas considerações adicionais sobre políticas comerciais também estão surgindo, relacionadas à regulamentação do fluxo de dados, conectividade digital e interoperabilidade[56].

De fato, ao reduzirem os custos de transação e possibilitarem a fragmentação das cadeias de produção, as tecnologias digitais e o livre fluxo de dados contribuíram decisivamente para o crescimento do comércio, especialmente de serviços, que tomam a forma de dados enviados através das fronteiras (OCDE, 2017, p. 232). Para COSTA (2016, p. 169 e 170):

> Além das questões relativas à propriedade intelectual, o mundo virtual também exacerbou a aplicação do Direito do Comércio Internacional. Uma vez que o ciberespaço permitiu a redefinição do contexto espaço-tempo, o comércio internacional que já vinha, desde a segunda metade do século XX, num movimento ascendente e sem retorno, rompeu de vez todas as barreiras nacionais e fronteiriças. O processo de negociação foi informatizado e quase todas as etapas comerciais são realizadas virtualmente, o que gerou um ponto de convergência entre as duas aldeias jurídicas, o chamado "*e-business*".

[56] Tradução livre do original em inglês: "Digitalisation has not only changed how we trade but also what we trade: a larger number of smaller and low-value packages of physical goods, as well as digital services are now crossing borders; goods are increasingly bundled with services; and new, and previously non-tradable, services are now being traded across borders. In this context, negotiating market access and behind-the-border measures continue to be trade policy priorities; digital trade still involves goods and services crossing borders and the applications of differing national regulations. But additional trade policy considerations are also emerging, related to data flow regulation, digital connectivity and interoperability".

Assim, ao mesmo tempo em que facilita a comercialização internacional de bens e serviços tradicionais, a transformação digital possibilitou o surgimento de novos modelos de negócios, dando ensejo ao desenvolvendo pela doutrina de uma tipologia do comércio digital. Para MELTZER (2016, p. 6):

> As economias estão se tornando digitais como a Internet e a capacidade de mover dados globalmente permitiu o desenvolvimento de negócios novos e inovadores. As cadeias de suprimentos globais também são possíveis pelo imenso fluxo de dados nas redes privadas e públicas. A Internet está transformando a maneira como os bens e serviços são usados e entregues, pois as empresas oferecem serviços on-line (como monitoramento de equipamentos ou análise de dados do uso de produtos) em combinação com bens, de modo que o componente de serviços seja uma parcela cada vez mais significativa dos valor geral do produto[57].

GONZÁLEZ e JOUNJEAN (2017) propõem uma tipologia em quatro categorias distintas de transação: bens e serviços estrangeiros adquiridos através de um intermediário online também estrangeiro; bens e serviços estrangeiros adquiridos através de um intermediário online nacional; bens e serviços nacionais adquiridos através de um intermediário online estrangeiro; e bens e serviços nacionais adquiridos através de um intermediário online também nacional, mas de propriedade de um estrangeiro.

CIURIAK e PTASHKINA (2018) consideram a existência de cinco diferentes modos de comércio digital. O denominado “Modo 1” se refere a produtos digitais que são baixados ou acessados através de streaming ou na “nuvem”, a exemplo de pesquisas na web (*Google*), *e-learning*, jogos *online*, aplicativos móveis (*app economy*), serviços de comunicação (*WhatsApp, Telegramm, Skype*), serviços de informações (*Google Maps*, *Waze*), publicidade online, *Netflix*, etc.

O segundo modo de comércio digital compreende o comércio de bens e serviços proporcionados pela digitalização da economia. É o que os autores denominam *Real to Real business to household (B2H) and business to business*

[57] Tradução livre do original em inglês: “Economies are going digital as the Internet and the ability to move data globally have enabled the development of new and innovative businesses. Global supply chains are also made possible by the immense flow of data across private and public networks. The Internet is transforming how goods and services are used and delivered, as businesses offer online services (such as monitoring of equipment or data analysis of product use) in combination with goods, such that the services component is an increasingly significant share of the overall product value”.

transactions with digital intermediation, isto é, negócios envolvendo bens e serviços “reais”, realizados entre comerciantes e consumidores finais, mas que somente se tornaram possíveis pelo desenvolvimento e massificação da internet, como aqueles desenvolvidos pela *Amazon*.

O “Modo 3” diz respeito às transações *peer-to-peer* (“de pessoa a pessoa”) realizadas através de aplicativos como *eBay*, *Uber* e *AirBnB*. De modo semelhante, o “Modo 4” se refere a um novo modelo de negócio denominado de *freelancers network*, impulsionado pelo surgimento de plataformas destinadas a conectar prestadores de serviços (*freelancers*, trabalhadores autônomos) e empresas, como a *Fiverr* e *Upwork*. O quinto e último modo de comércio digital, diretamente relacionado ao tema objeto do presente estudo, refere-se à capitalização do fluxo de dados.

Assim, medidas que afetem a capacidade de armazenamento, utilização e transferência de dados, principalmente através das fronteiras nacionais, são particularmente relevantes para o comercio internacional (CASALINI e GONZÁLEZ, 2019, p. 11), pois, atualmente, firmas de todos os tamanhos e setores da economia utilizam dados, e com a adoção de novos modelos de negócios, é improvável a realização de uma transação comercial internacional sem qualquer troca de informações entre as partes envolvidas (CASALINI e GONZÁLEZ, 2019, p. 13).

Nesse contexto, a crescente importância dos dados para a economia digital tem uma implicação crucial: os dados precisam ser movimentados através das fronteiras nacionais, pois muitas das inovações tecnológicas dependem dos fluxos internacionais de dados.

Essa interdependência coloca as políticas comerciais sob pressão e exige soluções claras. A proteção insuficiente pode criar efeitos negativos no mercado, reduzindo a confiança do consumidor, e a proteção excessivamente rigorosa pode restringir indevidamente os negócios, resultando em efeitos econômicos adversos.

2. PROTEÇÃO E TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

2.1. Aspectos gerais

Durante as décadas de 1970 e 1980, ainda nos primeiros anos da internet, a circulação de informação se dava, basicamente, entre redes fechadas de computadores de universidades e órgãos governamentais, especialmente nas áreas militar e de inteligência[58], e dentro das fronteiras nacionais (KUNER, 2013, p. 38 e 39).

Isso porque, a internet não teve origem no mundo dos negócios, mas em torno de centros acadêmicos e de pesquisa e de instituições governamentais. De fato, a criação e o desenvolvimento da internet, especialmente nas três últimas décadas do século XX, foram consequência da fusão de estratégia militar, grande cooperação científica, iniciativa tecnológica e inovação contracultural.

Segundo CASTELLS (2003, n. p.), "[A]s empresas não podiam se permitir fazer o longo desvio que seria necessário para estimular aplicações lucrativas de um esquema tão audacioso", pois a internet "[E]ra uma tecnologia ousada demais, um projeto caro demais, e uma iniciativa arriscada demais para ser assumida por organizações voltadas para o lucro", de modo que apenas os governos e as grandes corporações tinham condições de, já naquela época, beneficiarem-se da transferência de dados entre redes de computadores (KUNER, 2013, p. 38).

---

[58] Importante relembrar que a internet surgiu e se desenvolveu no contexto econômico, político e militar da Guerra Fria, período histórico (1945 a 1991) de disputas estratégicas e conflitos indiretos de ordem política, militar, tecnológica, econômica, social e ideológica entre os Estados Unidos e a extinta União Soviética e suas zonas de influência entre os Estados Unidos e a União Soviética, o que explica o importante papel desempenhado pelas áreas militar e de inteligência, principalmente do governo americano, no constante aprimoramento da tecnologia. De acordo com CASTELLS (2003, n. p.), "[A] despeito de toda a visão e de toda a competência que manifestaram em seu projeto, esses cientistas jamais teriam podido dispor do nível de recursos necessário para construir uma rede de computadores e para projetar todas as tecnologias apropriadas. A Guerra Fria forneceu um contexto em que havia forte apoio popular e governamental para o investimento em ciência e tecnologia de ponta, particularmente depois que o desafio do programa espacial soviético tornou-se uma ameaça à segurança nacional dos EUA. Nesse sentido, a Internet não é um caso especial na história da inovação tecnológica, um processo que geralmente está associado à guerra: o esforço científico e de engenharia feito em torno da Segunda Guerra Mundial constituiu a matriz para as tecnologias da revolução da microeletrônica, e a corrida armamentista durante a Guerra Fria facilitou o seu desenvolvimento".

Dessa forma, no âmbito empresarial, o fluxo internacional de dados se limitava a trocas pontuais de informações estritamente necessárias ao desenvolvimento regular das atividades econômicas (KUNER, 2013, p. 31), através sistemas internos de comunicação das próprias corporações ou grupos econômicos.

Nos últimos anos[59], no entanto, tem-se verificado uma profunda alteração naquele cenário, com o crescimento exponencial do volume de dados transferidos através das fronteiras nacionais, tendo sido publicados vários estudos destacando a importância dos fluxos internacionais de dados. De acordo com KUNER (2013, p. 158):

> Antes do início do uso generalizado da internet nos anos 90, supunha-se que os fluxos internacionais de dados fossem uma ocorrência excecional, e muitos dados transferidos eram técnicos e não pessoais. A situação mudou completamente, de modo que, ao invés de exceção, as transferências internacionais de dados pessoais tornaram-se a regra[60].

Segundo a UNCTAD (2015), em 2013, o comércio eletrônico *Business to Business* (B2B) foi estimado em US$ 15 trilhões. Nesse mesmo período, o comércio eletrônico *Business to Consumer* (B2C) foi muito menor, movimentando cerca de US$ 1,2 trilhão, mas estava crescendo rapidamente, especialmente nos países em desenvolvimento. O estudo observa, ainda, que a maioria do comércio eletrônico é nacional, embora o comércio digital internacional esteja crescendo rapidamente.

Da mesma forma, o *Brookings Institute* (2014) identificou que, em 2012, as exportações de serviços digitais pelos EUA totalizaram US$ 383,7 bilhões, ao passo que as importações foram de US$ 233,6 bilhões. Na União Europeia, os números foram de US$ 465 bilhões e US$ 297 bilhões, respetivamente.

---

[59] Ainda em 1990, a criação da world wide web (www) pelos pesquisadores Tim Berners-Lee e Robert Cailliau, do Centro Europeu para Pesquisa Nuclear (CERN, do francês *Centre Européen pour Recherche Nucleaire*), permitiu a difusão da internet para a sociedade em geral, ao possibilitar a organização do conteúdo de sites por informação, e não por localização, oferecendo aos usuários um sistema de pesquisa mais eficiente para as informações desejadas. Durante esse período, muitos provedores de serviços da internet montaram suas próprias redes e estabeleceram suas próprias portas de comunicação para fins comerciais. A partir de então, a internet cresceu rapidamente como uma rede global de redes de computadores.

[60] Tradução livre do original em inglês: “Before widespread use of the Internet began in the 1990s, it was assumed that transborder data flows were an exceptional occurrence, and many data transferred were technical and not personal. The situation has come full circle, so that instead of being the exception, transborder data flows of personal data are now the rule”.

De acordo com o MGI (2016), em 2014, aproximadamente US$ 30 trilhões em bens, serviços e finanças foram transferidos através das fronteiras nacionais. Estima-se que cerca de 12% do comércio internacional de mercadorias é realizado através de plataformas globais de comércio eletrônico. A dimensão internacional desses fluxos aumentou o PIB global em aproximadamente 10%, equivalente a um valor de US$ 7,8 trilhões em 2014. Os fluxos de dados representam aproximadamente US$ 2,8 trilhões desse valor agregado.

Para PORGES e ENDERS (2016, p. 1), há três categorias de fluxos internacionais de dados: a primeira categoria compreende informações e outros dados empresariais, incluindo dados pessoais, que dão suporte à produção, ao marketing, às vendas, ao pós-venda; a segunda, a exportação e a importação de bens e serviços digitais, bem como de mercadorias adquiridas eletronicamente (*e-commerce*); a terceira, a exportação e importação de conteúdo digital, incluindo *softwares*, música e conteúdo audiovisual. Para eles:

> Nossa opinião é de que as instituições políticas devem enfrentar obstáculos aos fluxos de dados transfronteiriços como uma questão prioritária. No século 21, todas as empresas que negociam dependem da capacidade de mover dados. Toda empresa que possui escritório, cliente, fornecedor ou contratado fora do país de origem depende do acesso transfronteiriço aos dados. Como aponta Rentzhog (2015), a manufatura moderna, a maioria dos produtos comercializados e muitos serviços essenciais simplesmente não podem funcionar sem um componente digital. Como corolário, não há maneira mais segura de interromper o comércio e prejudicar uma economia nacional do que restringir os fluxos de dados[61].

Dentre as diferentes razões tecnológicas, econômicas, sociais, culturais e políticas desse fenômeno, KUNER (2013, p. 32-34) destaca o aprofundamento da globalização econômica; o crescimento dos serviços de processamento de dados; a ubiquidade das transferências internacionais de dados; a importância cultural e social das atividades online; a maior participação dos próprios indivíduos nas transferências internacionais de dados; o aumento das transferências internacionais de dados

[61] Tradução livre do original em inglês: “Our view is that policy institutions must address obstacles to cross-border data flows as a priority matter. In the 21st century, all enterprises that trade depend on the hability to move data. Every company that has an office, a costumer, a supplier, or a contractor outside its home country depends on cross-border access to data. As Rentzhog (2015) points out, moderns manufacturing, most goods trade, and many essential services simply cannot function without a digital component. As a corollary, there is no surer way to stop trade and handicap a national economy than to cripple data flows.”

realizadas por Estados e organismos internacionais; e a perda da importância das fronteiras nacionais dos pontos de vista econômico e tecnológico.

Não obstante a aparente simplicidade com que as normas sobre proteção de dados pessoais definem transferência internacional de dados, KUNER (2013, p. 10 e 159) alerta para a falta de uniformidade das expressões utilizadas pelas normas e de clareza do seu significado. Segundo o autor:

> Há uma confusão sobre o que constitui "fluxos transfronteiriços de dados", e outras questões relacionadas, como a definição de dados pessoais e a distinção entre responsáveis pelo tratamento e subcontratantes de dados. Na prática, isso significa que esses termos são construídos de forma ampla, a fim de evitar o surgimento de lacunas na proteção.[62-63]

A LGPD (art. 5º, XV) utiliza a expressão "transferência internacional de dados", assim considerada "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro". A GDPR (Artigo 44º) se refere à "transferência para um país terceiro ou uma organização internacional". A OCDE, em suas *Privacy Guidelines* (§1º, "c"), utiliza a expressão "fluxo transfronteiriço de dados pessoais" para se referir ao "movimento de dados pessoais através das fronteiras nacionais"[64]. A *APEC CBPR System*, embora pensada com o objetivo e desenvolver um sistema de normas sobre privacidade aplicável à toda região da APEC, não define transferência internacional de dados; já a *APEC Privacy System* utiliza diversas expressões indistintamente ("fluxo de informações através das fronteiras"; "transferência internacional"; "fluxo transfronteiriço de informações"; "transferência transfronteiriça de dados"), também sem precisar os seus significados (KUNER, 2013, p. 10).

---

[62] Tradução livre do original em inglês: "There is confusion about what constitute 'transborder data flows', as well as concerning related questions such as how to define personal data and what the distinction should be between data controllers and data processors. In practice, this meant that such terms are broadly construed, in order to avoid creating gaps in protection".

[63] A tradução literal das expressões "data controllers" e "data processors" é "controladores de dados" e "processadores de dados", respectivamente. No entanto, optou-se por utilizar, na tradução, as expressões "responsáveis pelo tratamento" e "subcontratantes", tal qual a versão oficial em língua portuguesa do GDPR (Artigo 4º, ns. 7 e 8), disponibilizada em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. No Brasil, a LGPD utiliza as expressões "controlador" e "operador" (art. 5º, VI e VII), para significar a quem compete a tomada de decisões sobre o tratamento de dados pessoais e a realização do tratamento de dados pessoais em nome do controlador, respectivamente.

[64] Tradução livre do original em inglês: "'Transborder flows of personal data' means movements of personal data across national borders".

Para KUNER (2013, p. 11), a maior dificuldade em se definir transferência internacional de dados está no fato de que, muitas vezes, tais dados não são efetivamente transferidos para outros países ou organismos internacionais, mas simplesmente disponibilizados na internet, podendo ser acessados por terceiros localizados fora do território nacional do país de origem dos dados.

Ainda segundo KUNER (2013, p. 11), as normas tendem a considerar transferência internacional de dados com um único ato de vontade do agente, e não como parte de um processo bem mais complexo e que envolve várias etapas.

Nesse sentido, de acordo com SEN (2018, p. 4 e 5), o movimento dos dados através das fronteiras nacionais ocorre em quatro etapas. Primeiramente, os dados sempre surgem num dispositivo físico. Na segunda etapa, os dados são movimentados online através dos mecanismos da internet, em pequenas unidades denominadas “pacotes”. No terceiro estágio, os dados são armazenados fisicamente[65] em servidores localizados em *data centers*. No quarto e último estágio, os dados viajam dos servidores através de provedores de serviços de internet para os dispositivos dos usuários finais[66].

No Acórdão de 6 de novembro de 2003 (C-101/01, EU:C:2003:596), o TJUE entendeu que não ocorre uma transferência internacional de dados quando uma pessoa natural, localizada num Estado Membro, insere dados pessoais em

---

[65] SEN (2018, p.4) esclarece que, mesmo quando se utiliza computação na nuvem (*cloud computing*), os dados sempre são armazenados em servidores físicos.

[66] Esse caminho dos dados através das redes também é tratado por CASTELLS (2016, p. 108 e 109): “Assim, o poder de processamento, os aplicativos e dos dados ficam armazenados nos servidores de rede, e a inteligência da computação fica na própria rede: os sítios da web se comunicam entre si e têm à disposição o software necessário para conectar qualquer aparelho a uma rede universal de computadores (...). Além disso, o extraordinário aumento da capacidade de transmissão de tecnologia de comunicação em banda larga proporcionou a oportunidade de se usar a internet, ou tecnologia de comunicação semelhantes à internet, para transmitir voz, além de dados, por meio da troca de pacotes, o que revolucionou as telecomunicações e sua respectiva indústria. Segundo Vinton Cerf [matemático e informático estadunidense, referenciado como um dos fundadores da internet], ‘Hoje em dia é preciso passar por uma comutação de circuitos para obter uma troca de pacotes. No futuro, passaremos por uma troca de pacotes para obter uma comutação de circuitos’. Em outra previsão tecnológica, Cerf afirmou que ‘durante a segunda metade da próxima década – entre 2005 e 2010 – haverá um novo impulsionador (tecnológico): bilhões de aparelhos ligados à internet. Por fim, então, a rede de comunicação será a troca de pacotes, com a transmissão de dados sendo a responsável pelo espantoso compartilhamento de tráfego, e a transmissão de voz será apenas um serviço especializado. Esse volume de tráfego de comunicação exigirá uma expansão gigantesca da capacidade, tanto transoceânica quanto local. A criação de uma nova infraestrutura global de telecomunicações com fibra óptica e transmissão digital estava bem encaminhada em fins do século [XX], com capacidade de transmissão dos cabos de fibra óptica aproximando-se dos 100 gigabits por segundo no ano 2000, em comparação com os cerca de 5 gigabits em 1993”.

determinado site hospedado no âmbito da União Europeia, tornando-os, desse modo, acessíveis a terceiros, pessoa natural ou jurídica, localizados ou não dentro do bloco europeu. O TJUE considerou, ainda, que não seria possível presumir a intenção do legislador comunitário de incluir no conceito de transferência internacional de dados pessoais a inserção de dados pessoais em sites da internet, mesmo que tal inserção possibilitasse o seu acesso por pessoas de países terceiros, pois isso implicaria a necessidade de aplicação da legislação europeia sobre proteção e transferência internacional de dados pessoais a todos os indivíduos e empresas do mundo.

Por fim, é preciso diferenciar "transferência internacional de dados" do chamado "mero trânsito", definido por KUNER (2013, p. 15) como "situações em que os dados são roteados através de um país a caminho de outro"[67]. No Parecer 08/2010 sobre a lei aplicável, o Grupo de Proteção de Dados do Artigo 29º[68] exemplifica "mero trânsito" com os casos das redes de telecomunicações (cabos) e dos serviços postais, que apenas asseguram o trânsito das comunicações pela União Europeia, para depois chegarem aos destinatários finais, localizados fora do bloco.

2.2. Desafios no desenvolvimento e implementação das normas sobre proteção de dados pessoais

Existem vários desafios para o desenvolvimento e implementação das normas de proteção de dados. Em primeiro lugar, há claras divergências entre os sistemas legais, pois a abordagem da privacidade e proteção de dados pessoais varia conforme a cultura, sendo esse um dos motivos pelos quais há diferenças substanciais entre as regulações nacionais (CASALINI e GONZÁLEZ, 2019, p. 13).

[67] Tradução livre do original em inglês: "(...) situations where data are routed through one country on their way to another one".
[68] Grupo de Proteção de Dados do Artigo 29º (*Article 29 Working Party*) é um corpo consultivo composto por autoridades de proteção de dados dos Estados Membros, pela Comissão Europeia e pela Autoridade Europeia de Proteção de Dados.

Na União Europeia, a privacidade e a proteção dos dados pessoais possuem estatura de direitos humanos fundamentais[69 - 70]. Nesse sentido, o Artigo 8º da Convenção Europeia dos Direitos Humanos (CEDH) assegura a todos o direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência, ressalvada a excepcional possibilidade de ingerência pelo poder público, desde que prevista em lei e necessária à segurança nacional ou pública, à garantia do bem-estar econômico, à defesa da ordem e prevenção das infrações penais, à proteção da saúde ou da moral, ou à proteção dos direitos e das liberdades de terceiros. O direito à liberdade de expressão, que compreende "a liberdade de opinião e a liberdade de receber ou de transmitir informações ou ideias sem que possa haver ingerência de quaisquer autoridades públicas e sem considerações de fronteiras", está expressamente previsto no Artigo 10º da CEDH.

A Carta dos Direitos Fundamentais também protege a vida privada e familiar (Artigo 7º), incluindo a inviolabilidade do domicílio e das comunicações, mas vai além, em seu Artigo 8º, ao expressamente estabelecer que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito, os quais devem ser objeto de um tratamento leal, para fins específicos e mediante o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei.

Por outro lado, nos Estados Unidos, a proteção de dados pessoais recebe proteção apenas no contexto das relações gerais de consumo. Como os serviços digitais são bastante importantes para a balança comercial americana[71] (SELBY, 2017, p. 215), os Estados Unidos se tornaram, nos últimos anos, um grande defensor do livre fluxo de dados.

---

[69] Embora seja possível identificar referências à existência e proteção de um direito à dignidade, personalidade e autodeterminação em alguns sistemas constitucionais nacionais antes da Segunda Guerra Mundial, somente após esse conflito é que se pode falar no desenvolvimento de um sistema supranacional de direitos fundamentais (SCHWARTZ e PEIFER, 2017, p. 123), cujos pilares são a Convenção Europeia dos Direitos Humanos (CEDH) e a Carta dos Direitos Fundamentais da União Europeia.

[70] SCHWARTZ e PEIFER (2017, p. 126) apontam que os direitos fundamentais à privacidade e proteção de dados pessoais produzem "efeitos horizontais", ou seja, não se aplicam apenas ao poder público, alcançando também pessoas naturais e empresas.

[71] SELBY (2017, p. 215 e 216) destaca as razões da vantagem comparativa dos Estados Unidos em relação à prestação de serviços digitais: **(a)** berço do surgimento e desenvolvimento da internet, as empresas americanas saem na frente das concorrentes em relação às novas tecnologias; **(b)** a própria economia doméstica oferece uma enorme base de consumidores, que permite às empresas escalarem os seus serviços; **(c)** grande concentração de fundos e experiência; **(d)** as principais empresas de hospedagem de conteúdo digital são sediadas nos Estados Unidos.

Uma outra questão fundamental é que ainda existem lacunas na cobertura e aplicação das normas sobre proteção de dados. De acordo com o *UNCTAD Global Cyberlaw Tracker* [72], 58% dos estados membros possuem legislação sobre proteção de dados e privacidade; 10% possuem projetos de lei pendentes de aprovação; 21% não possuem qualquer legislação sobre a matéria[73].

Nos países em que não há legislação sobre a matéria, os dados pessoais recebem baixos níveis de proteção, reduzindo a confiança em uma ampla gama de atividades comerciais. Esses países também correm o risco de serem excluídos das oportunidades de comércio internacional, porque muitas transações comerciais exigem transferências internacionais de dados sujeitas a requisitos legais mínimos.

No entanto, a elaboração e implementação de leis de proteção de dados é um processo demorado e desafiador, devido à necessidade de conscientização e conhecimento técnico entre os legisladores e o judiciário (UNCTAD, 2016, p. 8).

Por outro lado, mesmo nos países em que há normas sobre proteção de dados pessoais, é comum a previsão de inúmeras regras de exceção quanto à aplicabilidade das normas, seja quanto ao titular de dados (por exemplo, apenas para crianças ou não para dados de funcionários); à natureza dos dados (por exemplo, apenas dados confidenciais, como registros médicos ou financeiros); à origem de dados (por exemplo, restritas à coleta de dados *online* ou *offline*); ou ao setor dos dados (por exemplo, isenções relacionadas ao setor público e privado ou leis restritas a setores específicos, como saúde e crédito).

Outro desafio é que a proteção de dados é um campo dinâmico e constantemente desafiado e influenciado pelos avanços da tecnologia e inovação. Segundo KUNER (2013, p. 174), "[A] Internet e outras tecnologias dificultaram a aplicação das normas sobre transferência internacional de dados, as quais deveriam levar a tecnologia melhor em consideração"[74], razão pela qual o autor defende a

---

[72] O UNCTAD Global Cyberlaw Tracker é o primeiro mapeamento global de leis cibernéticas (https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx). Ele rastreia legislações sobre comércio eletrônico, defesa do consumidor, proteção de dados e privacidade e crimes cibernéticos nos 194 estados membros da UNCTAD, indicando se um determinado país possui ou não legislação específica ou se há projetos de lei pendentes de aprovação.

[73] Em 12% dos casos não foi possível obter informações sobre a existência ou não de legislação ou projetos de lei relativos à privacidade e proteção de dados.

[74] Tradução livre do original em inglês: "The Internet and other technological developments have complicated the application of transborder data flow regulation, which should better take technology into account".

adoção de instrumentos contratuais de proteção, mais flexíveis, em detrimento de aprovações estatais prévias, sendo essa a única maneira de as normas sobre proteção e transferência internacional de dados acompanharem os avanços tecnológicos e nos modelos de negócios:

> Essas considerações levam à conclusão de que nos instrumentos internacionais e leis nacionais, a utilização de mecanismos como aprovações regulatórias e a apresentação de formulários de inscrição e registro deve ser desencorajada; instrumentos flexíveis como códigos de conduta e auditorias devem ser incentivados; e os reguladores devem ter amplos poderes de execução. Esse é a única forma de a regulação das transferências internacionais de dados acompanharem os avanços em tecnologia e negócios[75].

Os desafios impostos pelo rápido desenvolvimento tecnológico e pela globalização para a proteção de dados pessoais também são destacados por SCHWARTZ (2013, p. 1993). Para o professor de direito da *UC Berkeley School of Law*, as novas tecnologias facilitaram o processo de coleta de dados pessoais, que ocorre de forma cada vez mais automatizada e imperceptível aos seus titulares, além de ter aumentado a exposição de informações numa escala sem precedentes.

Recentes escândalos de vazamento e utilização indevida de dados pessoais, como o da *Cambridge Analytica*[76] e do Serviço Federal de Processamento de Dados (SERPRO)[77], reforçam a necessidade de discussão e regulação sobre a proteção de dados pessoais em uma sociedade cada vez mais tecnológica, globalizada e fundada em dados.

Nesse contexto, um dos objetivos dos novos marcos legais brasileiro e europeu é dar uma resposta apropriada aos rápidos avanços tecnológicos e à globalização, que trouxeram novos níveis de escala da coleta e de compartilhamento de dados pessoais, inclusive transferidos internacionalmente.

---

[75] Tradução livre do original em inglês: “These considerations lead to the conclusions that in international instruments and national laws, mechanisms such as regulatory approvals and the filing of application and registration forms should be disfavoured; flexible instruments like codes of practice and targeted audits should be encouraged; and regulators should be given enhanced enforcement powers. This is the only way that the regulation of transborder data flows has a chance of keeping up with advances in technology and business processes”.

[76] https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml

[77] https://www.conjur.com.br/2018-mai-31/mp-df-acusa-empresa-publica-vender-dados-brasileiros

A preocupação com os impactos das novas tecnologias em matéria de proteção e circulação de dados, num contexto em que a integração econômica e social resultante do funcionamento do mercado interno intensificou a transferência de dados pessoais dentro da própria União Europeia, é um dos fatores que levaram à mudança do marco regulatório da privacidade na União Europeia, conforme se infere dos itens 6 e 7 do preâmbulo do GDPR:

> (6) A rápida evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais. A recolha e a partilha de dados pessoais registaram um aumento significativo. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social e deverão contribuir para facilitar a livre circulação de dados pessoais na União e a sua transferência para países terceiros e organizações internacionais, assegurando simultaneamente um elevado nível de proteção dos dados pessoais.
>
> (7) Esta evolução exige um quadro de proteção de dados sólido e mais coerente na União, apoiado por uma aplicação rigorosa das regras, pois é importante gerar a confiança necessária ao desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares deverão poder controlar a utilização que é feita dos seus dados pessoais. Deverá ser reforçada a segurança jurídica e a segurança prática para as pessoas singulares, os operadores econômicos e as autoridades públicas.

No Brasil, o Parecer nº 64 da Comissão de Assuntos Econômicos do Senado Federal, de relatoria do Senador Ricardo Ferraço, favorável à aprovação da chamada LGPD, reconheceu que os impactos dos avanços tecnológicos na sociedade potencializaram a necessidade de instituição do marco regulatório da proteção de dados no país:

> O nível de avanço tecnológico a que a humanidade chegou permite o processamento massivo de dados, baseado em tecnologia digital avançada. E esse processamento já ocorre com base em inteligência artificial e algoritmos complexos, capazes de, por um lado, facilitar o processo produtivo de tomada de decisões empresariais, e, por outro lado, afetar a vida do cidadão.
>
> Podemos não ter consciência disso, mas tudo o que fazemos é coletado e armazenado em bases de dados cada vez maiores: ao acordarmos, usamos o celular ou tablet para as atividades cotidianas, como verificar mensagens, ler notícias na internet, conferir o clima e checar o nível de trânsito até o local de trabalho ou a escola dos filhos.
>
> Ao sair de casa, as torres de telefonia celular registram nosso itinerário. Aplicativos baseados em geolocalização monitoram nossos trajetos e traçam

> rotas do dia a dia. Programas instalados em nossos carros, telefones ou computadores registram nossos hábitos, gostos e preferências.
>
> Há aplicativos que monitoram com quem falamos por ligações telefônicas, vídeo-chamada ou mensagens de texto registrando data, hora e duração da chamada. Às vezes, até o conteúdo.
>
> Tudo é mensurável em dados, que podem revelar quem somos.

Percebe-se, assim, que, embora reconheçam a importância das novas tecnologias, a relação quase orgânica existente entre elas e os cidadãos, destacada pelo Parecer, representa um ponto comum de preocupação dos legisladores brasileiros e europeus, com influência direta na elaboração do GDPR e da LGPD.

As transferências internacionais de dados são cada vez mais importantes para o comércio, inovação e concorrência. Embora exista um consenso de que o fluxo de dados não pode ser completamente irrestrito, as diferentes regulações existentes não são universalmente adotadas.

A determinação da jurisdição também se tornou uma questão importante na regulamentação de proteção de dados, devido aos fluxos internacionais de dados e à falta de um único acordo global sobre proteção de dados (e a consequente fragmentação da regulamentação de proteção de dados).

2.3. Retórica da regulação e sua crítica

A regulação da proteção e transferência internacional de dados se relaciona com o conceito de “localização de dados”, que possui dois significados distintos[78] (SELBY, 2017, p. 214). Em primeiro lugar, trata-se da política regulatória que obriga os serviços de hospedagem de conteúdo digital a armazenarem os dados de seus usuários em servidores localizados dentro de determinada jurisdição. A segunda forma de localização de dados se refere à política regulatória que obriga os provedores de serviços na internet a rotearem os pacotes de dados enviados entre

[78] Além desses significados, também é possível classificar a localização de dados em ampla ou restrita. A primeira se aplica a todo e qualquer usuário ou tipo de dado; a segunda possui escopo mais limitado, aplicando-se a determinadas pessoas ou tipos específicos de dados (comumente financeiros e empresariais) (SELBY, 2017, p. 215).

usuários somente através de redes localizadas dentro de determinada jurisdição[79]. Nas palavras de SELBY (2017, p. 215):

> Nesse contexto, a localização de dados desafia os conceitos mencionados acima porque ela exige que os serviços de hospedagem de conteúdo digital construam ou aluguem *data centers* em determinadas jurisdições ao invés de poderem escolher onde quer que esses *data centers* sejam mais bem localizados (para otimizar sua performance econômica e/ou de rede[80].

Para CORY (2017, p 2), a localização de dados representa uma nova barreira ao comércio internacional, pois "[I]mpedir os fluxos de dados ou torna-los mais caros ou difíceis coloca as empresas estrangeiras em desvantagem. (...) Em essência, essa tática constitui 'protecionismo de dados' porque mantém concorrentes estrangeiros fora dos mercados domésticos"[81].

Os governos restringem e/ou condicionam o fluxo internacional de dados, incluindo a obrigatoriedade de armazenamento de dados dentro do território nacional, por inúmeros objetivos.

Segundo KUNER (2013, p. 158), num primeiro momento, a principal motivação para a elaboração de normas sobre proteção e transferência de dados pessoais era impedir o tratamento desses dados em países sem qualquer legislação sobre a matéria. Assim, a localização de dados protegeria a privacidade e segurança dos dados pessoais dos cidadãos.

Isso porque, se, por um lado, não se questiona a importância da transferência internacional de dados para o crescimento econômico, redução de custos de transação e melhoria da eficiência do processo produtivo, também é certo que, atualmente, o volume de dados movimentados diariamente por grandes corporações, especialmente as gigantes de tecnologia, governos e organismos internacionais e, até

---

[79] O presente estudo se refere apenas ao primeiro conceito de localização de dados e suas variantes, que incluem tanto a necessidade de armazenamento dos dados em determinada jurisdição quanto a imposição de requisitos/condições ao seu envio para outras jurisdições, culminando, no limite, com a vedação às transferências internacionais de dados.

[80] Tradução livre do original em inglês: "In this context, data localization challenges the first and second assumptions mentioned above because it requires Internet content hosts to build or rent data centres in specified jurisdictions rather than to be able to choose wherever those data centres might be most logically located (so as to optimize their economic and/or network performance)".

[81] Tradução livre do original em inglês: "These policies represent a new barrier to global digital trade. (...) In essence, these tactics constitute 'data protectionism' because they keep foreign competitors out of domestic markets".

mesmo, pelos próprios titulares[82] dos dados pessoais, expõe tais dados e a privacidade dos indivíduos a novos e maiores riscos (KUNER, 2013, p. 31 e 34).

Assim, a proteção da privacidade dos indivíduos, incluindo o controle sobre como seus dados pessoais são tratados (MITCHELL e MISHRA, 2019, p. 4), é uma das principais justificativas para a proliferação de normas sobre proteção de dados pessoais.

Nesse sentido, a justificativa constante do Projeto de Lei n° 4060/2012, que deu origem à LGPD, informa que "se faz necessário estabelecer normas legais para disciplinar tais relações [através da internet], especialmente para dar proteção à individualidade e à privacidade das pessoas, sem impedir a livre iniciativa comercial e de comunicação".

Outras medidas se relacionam à segurança nacional, seja em termos de proteção de informações consideradas sensíveis, seja para possibilitar às autoridades de segurança nacional o acesso e revisão de dados (CASALINI e GONZÁLEZ, 2019, p. 13). Defende-se, assim, que a localização de dados possibilita maior segurança contra agências de inteligência estrangeiras.

Também é possível identificar nas normas sobre proteção e transferência internacional de dados medidas de proteção e estímulo à indústria local. Isso reflete a visão de que os dados são um recurso que precisa estar disponível aos fornecedores e produtores nacionais (CASALINI e GONZÁLEZ, 2019, p. 13). O principal argumento é que os países em desenvolvimento são incapazes de se beneficiarem das cadeias globais de valor uma vez que a propriedade intelectual e dados importantes são predominantemente detidos por empresas sediadas em países desenvolvidos (MITCHELL, 2019, p. 8).

No entanto, é importante considerar o quão efetivas são as medidas mencionadas acima no atingimento de seus objetivos, os custos e *trade-offs* associados e se há medidas alternativas que possibilitariam um melhor equilíbrio entre tais objetivos para maximizar os benefícios para a população (CASALINI e GONZÁLEZ, 2019, p. 13).

---

[82] Nos termos do art. 5º, V, da Lei n° 13.709/2018, "titular" é a pessoa natural a que se referem os dados pessoais. O Regulamento (UE) 2016/279, o Regulamento Geral sobre a Proteção de Dados da União Europeia, possui definição semelhante em seu artigo 4° (1), segundo o qual "titular dos dados" é a pessoa natural identificada ou identificável a que se referem os dados pessoais.

CORY (2017, p. 4), por exemplo, considera que a localização dos dados não tem qualquer efeito sobre a privacidade e segurança dos dados pessoais dos indivíduos, pois isso depende dos controles técnicos, físicos e administrativos implementados, que podem ser fortes ou fracos, independentemente do local dos *data centers*. Para ele, "(...) legisladores não compreendem que a confidencialidade dos dados não depende, de modo geral, do país em que a informação está armazenada, apenas das medidas utilizadas para mantê-los seguros"[83].

Ademais, deve-se ressaltar que o armazenamento de dados em um determinado *data center* pode torna-lo um alvo em potencial para ciberataques; igualmente, uma vez que os países permanecem conectados à internet, os dados permanecem vulneráveis a ataques (MITCHELL e MISHRA, 2019, p. 6).

Relativamente à proteção e promoção da economia nacional, embora considere possível a redução da importação de serviços, pois empresas e usuários locais não teriam que pagar a empresas estrangeiras para hospedarem seus dados no exterior, SELBY (2017, p. 229) destaca a potencial ocorrência de um efeito colateral dessa medida, que pode simplesmente anular eventuais benefícios: o aumento da importação de máquinas e equipamentos necessários para construção e montagem de *data centers*, uma vez que:

> Como a maioria dos países não produzem seus próprios CPUs, placas-mãe, memória RAM, discos rígidos (sendo a China uma exceção óbvia), a imposição de localização de dados e a construção de data centers locais normalmente não reduz a demanda por importação de equipamentos eletrônicos[84].

Ademais, é possível que os *data centers* locais cobrem preços mais altos pela hospedagem de conteúdos digitais em razão da inexistência de um mercado local consolidado e da baixa demanda, aumentando, assim, os custos operacionais e, por conseguinte, reduzindo a competitividade internacional.

---

[83] Tradução livre do original em inglês: "(...) policymakers misunderstand that the confidentiality of data does not generally depend on which country the information is stored in, only on the measures used to store it securely".

[84] Tradução livre do original em inglês: "As most countries do not produce their own CPUs, motherboards, RAM chips, hard disks or network equipment (China being the obvious exception), requiring data localization and building local data centres does not typically reduce demand for imports of high-tech equipment".

Igualmente, CORY (2017, p. 5) considera tais medidas como uma "nova forma de 'mercantilismo digital'"[85]. Sob a perspectiva da criação de novos empregos, ele argumenta que, à medida que os *data centers* se tornam cada vez mais autorizados, o número de postos de trabalho, especialmente na área técnica, tende a diminuir[86], ainda que, num primeiro momento, durante à construção das instalações, esse número possa se mostrar superavitário.

2.4. Tipologia das abordagens regulatórias

O surgimento e o crescimento de modelos de negócios baseados em dados fizeram com que muitos países atualizassem suas legislações nacionais ou elaborassem regulação própria sobre a matéria, uma vez que, conforme observado por KUNER (2013, P. 158):

> Hoje, a regulação dos fluxos internacionais de dados é matéria de importância estratégica, na medida em que os fluxos de dados se tornaram parte integrante do desenvolvimento econômico e social, liberdade de expressão, atividades culturais, e ouros valores sociais básicos[87].

Em nível nacional, a disseminação geográfica de normas sobre proteção e transferência internacional de dados pessoais aumentou drasticamente. De acordo com o *UNCTAD Global Cyberlaw Tracker*, 107 países possuem legislação sobre proteção de dados.

Essa proliferação de normas levou a uma fragmentação jurídica, com o surgimento de diferentes tipos de regulação e de atores regionais e internacionais responsáveis pela sua aplicação (KUNER, 2013, p. 25), dando ensejo a novas abordagens regulatórias em matéria de proteção de dados pessoais, incluindo a obrigatoriedade de armazenamento de dados pessoais em servidores localizados no território do país de origem de tais dados e a imposição de restrições ou condições às transferências internacionais de dados.

---

[85] Tradução livre do original em inglês: "(...) a new form of 'digital mercantilism'".
[86] O autor menciona o *data center* da Apple, construído em 2011, que, a despeito de ter custado US$ 1 bilhão, criou apenas 50 empregos diretos e 250 indiretos.
[87] Tradução livre do original em inglês: "Regulation of transborder data flows is now a subject of strategic importance, as data flows have become integral to economic and social development, free expression, cultural activities, and other basic social values".

KUNER (2013, p. 157 e 158) observa que, desde o início dos anos 70, há uma crescente tensão entre aqueles que defendem a completa ausência de regulação ou que ela se limite ao estritamente necessário e os que consideram necessário regular detalhadamente as transferências internacionais de dados, a fim de permitir a livre circulação de informações. Trata-se, no entanto, segundo o próprio autor, com quem concordamos, de uma falsa dicotomia, uma vez que:

> Essa tensão entre o livre fluxo de dados e a regulação dos fluxos internacionais de dados é baseada numa falsa dicotomia. Permitir que os dados sejam livremente movimentados através das fronteiras nacionais é essencial para a liberdade de expressão, assim como para outros direitos e valores. Ao mesmo tempo, a crescente importância social e econômica dos fluxos de dados implica que tais devem continuar recebendo proteção quando transferidos[88].

A abordagem baseada em geografia visa proteger contra os riscos apresentados pelo local de destino dos dados, enquanto a abordagem baseada na organização visa os riscos apresentados pelas organizações que recebem os dados, responsabilizando os exportadores de dados por garantir a proteção contínua dos dados pessoais transferidos, independentemente da sua localização geográfica (KUNER, 2013, p. 64-76).

FERRACINI (2017) propõe uma classificação das abordagens regulatórias de acordo com o nível de restrição imposto pelos Estados. Numa primeira categoria, estão as condições estritas ao fluxo internacional de dados, compreendendo a imposição de obrigação de armazenagem, a imposição de obrigação de armazenagem combinada com a obrigação de processamento dos dados localmente e vedação às transferências internacionais de dados.

Quando um requisito de armazenamento local se aplica, os dados não podem ser transferidos para outros países, a menos que uma cópia seja armazenada dentro das fronteiras nacionais. Nesses casos, desde que uma cópia dos dados seja salva localmente, as atividades de armazenamento e processamento de dados também podem ocorrer fora do país. Além dos requisitos de armazenamento local, as

[88] Tradução livre do original em inglês: “This tension between the free flow of data and regulation of transborder data flows is based on a false dichotomy. Allowing data to flow freely across international borders is essential to freedom of expression, as well as to other important rights and values. At the same time, the increasing social and economic importance of data flows means that data should continue to receive protection when transferred”.

restrições também podem se estender ao processamento de dados. Isso significa que a empresa precisa usar *data centers* localizados no país para o processamento dos dados. O terceiro e mais rigoroso tipo de restrição aos fluxos internacionais de dados consiste na proibição de transferir os dados através das fronteiras. Portanto, os dados devem ser armazenados, processados e acessados no território do país de implementação.

Numa segunda categoria, estão as restrições condicionais aos fluxos internacionais de dados. Quando existe um regime de fluxo condicional, a transferência dos dados para o exterior é proibida, a menos que determinadas condições sejam cumpridas. As condições podem ser aplicadas ao país destinatário, à empresa ou ao país destinatário e à empresa. Na maioria dos casos, basta que uma das opções alternativas seja atendida para que a empresa transfira dados para o exterior. Se as condições forem rigorosas e não puderem ser cumpridas pelo país destinatário nem pela empresa, a medida resultará na proibição da transferência de dados para o exterior.

Também sob esse prisma, CASALINI e GONZÁLEZ (2019, p. 16-24) desenvolveram uma taxinomia das diferentes abordagens regulatórias em matéria de transferência internacional de dados pessoais, em sentido amplo, compreendendo tanto fluxo de dados através das fronteiras nacionais propriamente dito, quanto a obrigatoriedade de armazenamento desses dados em servidores localizados dentro do território nacional.

O fluxo internacional de dados é dividido em quatro categorias, levando em consideração o nível de restrição à movimentação dos dados através das fronteiras nacionais.

A primeira categoria se refere à completa ausência de regulação sobre a transferência internacional de dados. Segundo dados disponíveis na *UNCTAD Cyberlaw Global Tracker*, estão nessa categoria os cerca de 60 países que não possuem qualquer regulamentação sobre a matéria e aqueles que possuem projetos de lei em tramitação[89].

[89] Embora se reconheça a importância das iniciativas legislativas no sentido de regulamentar a matéria, o fato é que, do ponto de vista prático da proteção dos dados pessoais, não há diferença entre países que não possuem legislação e aqueles que já possuem projetos de lei em discussão: ambos não

Na segunda categoria (denominada pelos autores de fluxo livre) se enquadram as regulações que não proíbem nem estabelecem qualquer condição prévia as transferências internacionais de dados. Nesta hipótese, atribui-se ao controlador responsável pelo envio dos dados a responsabilidade pelo correto uso dos dados pessoais no país receptor.

A terceira categoria (fluxo condicionado a salvaguardas) compreende as legislações que se baseiam na noção de adequação[90] como condição para que os dados sejam transferidos. Tal categoria possui 3 subgrupos, que diferem entre si em como e por quem as "decisões de adequação" são aplicadas, e nas hipóteses de exceção em caso de não cumprimento do requisito de "adequação".

Na primeira subcategoria, a transferência internacional de dados é permitida quando o exportador de dados, com base em sua própria avaliação, entende que o país receptor oferece um nível adequado ou equivalente de proteção.

No entanto, mesmo que tal nível de proteção não esteja presente, ainda assim é possível realizar a transferência dos dados mediante o oferecimento de garantias contratuais [91] ou em determinadas hipóteses específicas, como a obtenção do consentimento[92] do titular dos dados; quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; quando a transferência for necessária para o interesse público; para o cumprimento de obrigação legal ou regulatória pelo controlador; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

---

possuem qualquer disciplina sobre fluxo internacional de dados, razão pela qual optou-se por considerar os dois cenários dentro da primeira categoria da classificação sugerida por Casalini e González.

[90] A noção de adequação está relacionada ao grau de proteção oferecido pelo país ou organismo internacional receptor dos dados pessoais.

[91] Os diferentes tipos de garantias contratuais (cláusulas contratuais específicas para determinadas transferências; cláusulas-padrão contratuais; normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos) serão detalhadas no tópico dedicado à análise das principais normativas nacionais e internacionais sobre transferência internacional de dados.

[92] Nos termos do art. 33, VIII, da LGPD, o consentimento deve ser específico e em destaque para a transferência, devendo conter informação prévia sobre o caráter internacional a operação, distinguindo-a claramente de outras finalidades. De modo semelhante, a GDPR (Artigo 49°) exige que o consentimento tenha sido explícito, após o titular dos dados ter sido informado dos possíveis riscos de tais transferências para si próprio devido à falta de uma decisão de adequação ou de garantias adequadas.

Embora confira maior flexibilidade às empresas, na medida em que delega aos particulares poderes de avaliação e decisão sobre a realização ou não da transferência internacional de dados, essa abordagem também aumenta os riscos das empresas, uma vez que elas se tornam responsáveis pelas transferências e eventuais violações aos direitos dos titulares.

Na segunda subcategoria, a avaliação se determinado país estrangeiro ou organismo internacional proporcionam um nível de proteção adequado, necessário à transferência internacional e dados, é feita pelo poder público, e não pelo setor privado. Da mesma forma, essa abordagem também prevê a possibilidade de a transferência internacional de dados ocorrer com fundamento em garantias contratuais ou desde que se verifiquem determinadas situações específicas, listada acima. Assim como ocorre com a decisão de adequação, o conteúdo e a forma das garantias contratuais também devem ser previamente aprovados pelo poder público.

No Brasil, compete exclusivamente à Autoridade Nacional de Proteção de Dados (ANPD)[93] avaliar o nível de proteção de dados do país estrangeiro ou do organismo internacional (art. 34) e definir o conteúdo de cláusulas-padrão contratuais, bem como verificar cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta (art. 35).

Na União Europeia, essas competências são repartidas entre a Comissão Europeia e as Autoridades de Controle Independentes, uma ou mais autoridades públicas independentes responsáveis pela fiscalização da aplicação da GDPR[94].

---

[93] A ANPD foi criada pela Lei n° 13.853/2019, resultado da conversão da Medida Provisória n° 869/2018. A ANPD foi criada como órgão da administração pública federal, integrante da Presidência da República (art. 55, *caput*, da LGPD). No entanto, a própria LGPD (art. 55, §§ 1° e 2°) prevê a possibilidade de a ANPD ser transformada em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. A avaliação quanto à transformação deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD, ainda sem cronograma definido. A ANPD é composta por um Conselho Diretor, órgão máximo de direção (composto de 5 diretores, escolhidos pelo Presidente da República e por ele nomeados, após aprovação pelo Senado Federal), pelo Conselho Nacional de Proteção de dados e Privacidade (composto por 23 representantes, titulares e suplentes), e por uma Corregedoria, uma Ouvidoria, um órgão de aconselhamento jurídico próprio e unidades administrativas e especializadas necessárias à aplicação da LGPD.

[94] Ainda durante a vigência da Diretiva 95/46/CE, no Acórdão de 9 de março de 2010 (C-518/07, EU:C:200:125), o TJUE declarou que a garantia de independência das autoridades nacionais de fiscalização visa assegurar a eficácia e a probidade da fiscalização. No Acórdão de 16 de outubro de 2012 (C-614/10, EU:C:2012:631), o TJUE afirmou que a expressão “com total independência” prevista

Compete à Comissão decidir se um país ou organismo internacional assegura um nível de proteção adequado, possibilitando as chamadas transferências com base numa decisão de adequação.

Relativamente às garantias contratuais, elas podem ser adotadas tanto pela Comissão quanto por uma Autoridade de Controle Independente, sendo que, neste último caso, sua forma e conteúdo devem ser submetidas à aprovação da Comissão pelo procedimento de exame previsto no artigo 5º do Regulamento (EU) n° 182/2011, que estabelece as regras e os princípios gerais relativos aos mecanismos de controle dos Estados-Membros do exercício das competências de execução.

Dessa forma, nessa segunda subcategoria, embora a avaliação sobre a existência de um nível adequado de proteção seja de competência do poder público, ainda assim é possível realizar a transferência internacional de dados, com fundamento em garantias contratuais ou outras situações excepcionais legalmente previstas.

A terceira subcategoria também prevê a participação direta do poder público, seja nas decisões de adequação, seja na definição do conteúdo e forma das garantias contratuais, bem como a possibilidade de os dados pessoais serem transferidos para outros países ou organismos internacionais com fundamento em alguma das hipóteses excepcionais previstas em lei.

---

no Artigo 28º, n. 1, da Diretiva 95/46/CE (correspondente ao Artigo 52º, n. 1, da GDPR), implica que as autoridades de controle devem gozar de uma independência que lhes permita exercer suas atribuições sem influência externa, de modo a evitar não apenas a influência direta, sob a forma de instruções, mas também qualquer forma de influência indireta suscetível de orientar as decisões das autoridades de controle. Nesse mesmo sentido, no Acórdão de 8 de abril de 2014 (C-288/12, EU:C:2014:237), o TJUE reafirmou sua jurisprudência no sentido de que a independência de que gozam as autoridades de controle exclui qualquer influência externa, sob qualquer forma, direta ou indireta, suscetíveis por em xeque o equilíbrio entre a proteção da vida privada e a livre circulação de dados pessoais. Além disso, entendeu que o mero risco de influência política nas decisões das autoridades de controle é suficiente para afastar a independência exigida direito europeu sobre proteção de dados pessoais.

Difere, no entanto, ao atribuir ao exportador dos dados a obrigação de assegurar que os dados transferidos receberão o mesmo tratamento[95-96] que eles teriam caso processados no país de origem, nas transferências realizadas apenas com fundamento em garantias contratuais ou nas situações especificas previstas em lei, isto é, quando não houver decisão de adequação proferida pelo poder público.

Por fim, a quarta categoria ("fluxo condicionado a autorizações *ad hoc*") compreende outras duas subcategorias. Em comum, o fato de haver apenas dois fundamentos para a realização de transferências internacionais de dados: uma decisão de adequação ou uma autorização específica (*ad hoc*) conferida pelo poder público. Diferem, no entanto, no fato de a segunda subcategoria exigir uma autorização específica em toda e qualquer transferência internacional de dados, mesmo para países ou organismos internacionais que possuam uma decisão de adequação vigente.

Relativamente à obrigatoriedade de armazenamento de dados pessoais em servidores localizados dentro do território nacional do país de origem, CASALINI e

---

[95] A definição de tratamento é bastante semelhante entre as diferentes legislações consultadas. A LGPD define tratamento como "toda operação realizada com dados pessoais, como as que se referem 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" (art. 5º, X); a GDPR, como "uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição"(Artigo 4º, n. 2).

[96] O TJUE já teve oportunidade analisar o conceito de tratamento de dados pessoais em duas oportunidades. No Acórdão de 6 de novembro de 2003 (C-101/021, EU:2003:596), o Tribunal de Recurso da Suécia questionou o TJUE se a publicação de dados pessoais (no caso, nomes, telefones, informações relativas a condições de trabalho etc) em sites criados em computador particular configura tratamento de dados pessoais sujeito à legislação sobre proteção de dados pessoais. Ao analisar a questão, o TJUE entendeu que a referência a pessoas e divulgação de informações sobre elas em sites da internet constitui um "tratamento de dados pessoais por meios total ou parcialmente automatizados", isto é, com base em inteligência artificial, não se enquadrando na exceção geral, prevista tanto no Brasil quanto na União Europeia, que afasta a aplicação das normas sobre proteção de dados pessoais aos tratamentos de dados pessoais realizados por pessoas naturais para fins exclusivamente particulares e não econômicos.

No Acórdão de 13 de maio de 2014 (c-131/12. Eu:C:2014:317), o TJUE entendeu que as atividades desempenhadas por buscadores (no caso, tratava-se do Google Spain e Google), isto é, encontrar informações publicadas na internet por terceiros, indexá-las, armazená-las e colocá-las à disposição de terceiros na internet, deve ser considerada "tratamento de dados pessoais" quando tais informações contenham dados pessoais, mesmos quando já publicados em outros meios de comunicação. No caso específico, o TJUE determinou que o Google Spain e o Google adotassem as medidas necessárias para retirar do seu índice e impossibilitar o acesso no futuro de anúncios publicados, em 1998, no jornal La Vanguardia, relativos à venda de imóveis em hasta pública em razão de arresto decorrente de dívidas de pessoa natural.

GONZÁLEZ (2019, p. 23) apresentam uma classificação dos diferentes regimes jurídicos em quatro categorias distintas, levando em consideração o nível de restrições impostas à livre circulação dos dados pessoais Estão compreendidas nesta categoria medidas que exigem que determinados tipos de dados sejam armazenados em servidores locais ou processados dentro do território nacional. Embora seja mais comum a imposição dessa obrigação para dados relativos a setores fortemente regulados (finanças, saúde, seguros, telecomunicação etc), é possível sua aplicação, também, aos dados pessoais, o que justifica a presente análise.

A primeira categoria se refere às legislações que não impõe qualquer obrigação de armazenamento ou processamento de dados pessoais no território nacional do país de origem. De acordo com CASALINI e GONZÁLEZ (2019, p. 23 e 24), trata-se da categoria mais comum, seja por ser pouco utilizada, seja porque, normalmente, limita-se a dados de setores específicos e por período limitado.

Na segunda categoria, exige-se que uma cópia dos dados seja armazenada em servidores locais, inexistindo qualquer empecilho à transferência para outros países ou organismos internacionais ou ao processamento realizado fora do território nacional. O principal objetivo desse tipo de regulação é facilitar o acesso do poder público a dados fiscal e de telecomunicação, especialmente, driblando, assim, eventuais problemas causados pela dificuldade de se obter informações armazenadas em outras jurisdições CASALINI e GONZÁLEZ (2019, p. 23 e 24), mesmo havendo acordos internacionais nesse sentido.

De forma semelhante, a terceira categoria também não impõe restrições ao fluxo internacional de dados. No entanto, veda o armazenamento dos dados fora do território nacional, de modo que os dados podem ser transferidos para outros países ou organismos internacionais, onde serão tratados, mas deverão retornar ao país de origem para armazenamento, tão logo o tratamento seja concluído.

A quarta e última categoria compreende as legislações que, além de imporem a obrigação de os dados serem armazenados localmente, estabelecem restrições ou condições à transferência internacional dos dados ou ao seu processamento fora do território nacional. Tal abordagem tem como objetivo proteger a economia local, estimulando o desenvolvimento de novos *data centers* e dos serviços de processamento de dados (CASALINI e GONZÁLEZ, 2019, p. 24).

2.5. Instrumentos internacionais

2.5.1. Organização para a Cooperação e Desenvolvimento Econômico (OCDE)

A discussão sobre os fluxos internacionais de dados começou na OCDE em 1970, culminando na publicação das Diretrizes de Privacidade da OCDE em 1980. As Diretrizes são um conjunto de princípios não vinculativos que os Estados Membros podem adotar e têm o duplo objetivo de alcançar a aceitação de certos padrões mínimos de privacidade e proteção de dados pessoais e de eliminar, na medida do possível, fatores que possam induzir os países a restringir o fluxo internacional de dados.

As Diretrizes contêm as seguintes disposições principais que tratam dos fluxos internacionais de dados: **(a)** os Estados Membros devem levar em consideração as implicações para outros países Membros no processamento doméstico e reexportação de dados pessoais; **(b)** os Estados Membros devem tomar todas as medidas razoáveis e apropriadas para garantir que os fluxos internacionais de dados pessoais, incluindo o trânsito através de um país membro, sejam ininterruptos e seguros; **(c)** os Estados Membros devem abster-se de restringir os fluxos internacionais de dados pessoais entre si e outro Estado Membro, exceto quando este último ainda não observar substancialmente essas Diretrizes ou onde a reexportação desses dados contornaria sua legislação doméstica sobre privacidade. Os Estados Membros também pode impor restrições em relação a certas categorias de dados pessoais para os quais sua legislação doméstica sobre privacidade inclui regulamentos específicos em vista da natureza desses dados e para os quais o outro Estado Membro não oferece proteção equivalente; **(d)** os Estados Membros devem evitar o desenvolvimento de leis, políticas e práticas em nome da proteção da privacidade e das liberdades individuais, o que criaria obstáculos aos fluxos internacionais de dados pessoais que excederiam os requisitos para tal proteção.

Para a UNCTAD (2016, p. 27), as Diretrizes possuem como pontes fortes o fato de terem uma história longa e respeitada; seus princípios básicos serem amplamente aceitos; concentrarem-se em alcançar o equilíbrio entre fluxos de dados e proteção de dados; e terem amplo apoio de um grupo diversificado. Por outro lado, verifica-se a ausência de um princípio de proporcionalidade (ou minimização de

dados); não possuem natureza vinculante; e representem a visão de mundo dos países desenvolvidos.

2.5.2. Convenção 108 do Conselho da Europa

A Convenção de Proteção de Dados do Conselho da Europa de 1981, geralmente referida como Convenção 108, é o acordo internacional vinculativo mais importante sobre proteção de dados. Embora a Convenção 108 tenha sido estabelecida pelo Conselho da Europa, sua adesão é aberta a qualquer país, inclusive fora do bloco europeu.

A Convenção 108 não cria direitos para indivíduos e não é diretamente aplicável a particulares, mas obriga os Estados a implementarem em suas leis as proteções que estabelece. No entanto, deixa considerável margem de manobra para os Estados implementarem suas disposições de diferentes maneiras, à luz de seus sistemas legais e constitucionais (KUNER, 2013, p. 76). A possibilidade de derrogação de suas disposições também enfraquece o regime jurídico de proteção de dados.

As regras gerais sobre transferências internacionais de dados estão contidas no artigo 12 da Convenção 108, com a seguinte redação:

> **Artigo 12 – Fluxos transfronteiriços de dados pessoais e lei doméstica**
> 1 As disposições seguintes aplicam-se à transferência através das fronteiras nacionais, por qualquer meio, de dados pessoais submetidos a processamento automático ou coletados com o objetivo de serem processados automaticamente.
> 2 Uma Parte não deverá, com o único objetivo de proteger a privacidade, proibir ou sujeitar a autorização especial fluxos transfronteiriços de dados pessoais que vão para o território de outra Parte.
> 3 Todavia, cada Parte terá o direito de derrogar o disposto no parágrafo 2:
> a) na medida em que sua legislação inclua regulamentos específicos para certas categorias de dados pessoais ou arquivos automatizados de dados pessoais, devido à natureza desses dados ou desses arquivos, exceto quando os regulamentos da outra Parte fornecerem uma proteção equivalente;
> b) quando a transferência for feita do seu território para o território de um Estado não contratante através do intermediário do território de outra Parte, a fim de evitar tais transferências que resultem em contornar a legislação da Parte mencionada no início deste parágrafo.

A despeito do seu viés eurocêntrico e da dificuldade em acomodar regimes jurídicos nacionais muito diferentes, a Convenção 108 possui vários pontos positivos, com destaque para sua cobertura abrangente; a ampla aceitação dos seus princípios;

possibilidade de adesão de terceiros; adoção de um processo aberto colaborativo; natureza vinculante do acordo, o que favorece a harmonização (UNCTAD, 2016, p. 25).

2.5.3. Organização Mundial do Comércio (OMC)

2.5.3.1. Aspectos gerais

O atual sistema multilateral de comércio, atualmente consolidado no âmbito da OMC, surgiu no período pós-Segunda Guerra Mundial, quando os líderes dos países ocidentais vencedores do conflito buscaram estabelecer mecanismos internacionais que evitassem a reedição de políticas nacionais individualistas marcadas pelo favorecimento de exportações e restrição de importações.

A partir do entendimento de que o crescimento das economias estava diretamente relacionado com a ampliação do comércio internacional, a ordem econômica internacional, pós-Segunda Guerra Mundial, foi estruturada com o objetivo de estabelecer uma unidade jurídico-econômica, dotada de previsibilidade e equidade, capaz de disciplinar a cooperação entre os países para a intensificação do comércio internacional.

As conferências de Bretton Woods (1944), redefinindo a arquitetura econômico internacional, estabeleceram as primeiras regras para as relações comerciais e financeiras entre os países. Sua realização se deu no contexto do pós-Segunda Guerra, momento em que a comunidade internacional estava empenhada em estabelecer uma maior integração global, principalmente em relação as questões econômicas.

Para regular aspectos financeiros e monetários, com o objetivo de garantir fixidez e unidade cambial nas trocas internacionais, foi instituído o Banco Internacional para Reconstrução e Desenvolvimento (BIRD), posteriormente dividido em Banco Mundial, Banco para Investimentos Internacionais e Fundo Monetário Internacional.

As principais disposições do Sistema Bretton Woods, em matéria financeira e monetária, foram a obrigação de cada país adotar uma política monetária que mantivesse a taxa de câmbio dentro de um determinado indexado ao dólar (americano), que, por sua vez, estaria ligado ao ouro em uma base fixa, e a provisão

pelo FMI de financiamento para suportar dificuldades temporárias de pagamentos pelos países.

No âmbito comercial, para disciplinar a regulação do comercio internacional pelos países, evitando a adoção de medidas protecionistas, foi projetada a criação da Organização Internacional do Comércio (OIC), que atuaria como uma agência das Nações Unidas, especializada em matéria de comércio internacional.

O foro para discussões e debates acerca da OIC ocorreu em Cuba, entre novembro de 1947 e março de 1948, resultando na assinatura da Carta de Havana, em que constava a criação da OIC.

A proposta da OIC demonstrava-se, à época, audaciosa, uma vez que, além de disciplinar o comércio internacional, estabelecia normas sobre trabalho, práticas restritivas ao comércio, investimentos internacionais e circulação de serviços e mão-de-obra.

No entanto, a criação da OIC, como organismo permanente de normatização e regulação do comércio internacional, não chegou a se concretizar, ficando prejudicada em razão da desistência dos Estados Unidos em encaminhar o projeto para ratificação pelo Congresso.

Fracassada a criação da OIC, foi firmado, em 1947, o Acordo Geral de Tarifas e Comércio (GATT-1947), que estabeleceu compromissos sobre tarifas e regras comerciais baseados nos acordos da OIC, com o objetivo de promover a progressiva liberalização do comércio internacional.

Assim como o Banco Mundial e o FMI, o GATT-1947 foi mais uma iniciativa internacional criada para, ao mesmo tempo, regular e integrar a economia global por meio do comércio.

Concebido com a finalidade de expandir o comércio internacional, o GATT-1947, originalmente criado para regular, provisoriamente, as relações comerciais internacionais, foi a base normativa para toda a experiência de trocas comerciais no âmbito internacional, disciplinando a matéria por mais de 40 anos.

Com o fracasso das negociações em torno da Carta de Havana, que, como visto, pretendia constituir a OIC, especialmente em razão da desistência norte-americana do projeto, o sistema multilateral de comércio foi desenvolvido através de uma série de negociações comerciais (denominadas “rodadas”) realizadas no âmbito

do GATT-1847, com o principal objetivo de promover a progressiva abertura comercial.

No âmbito do GATT-1947, foram realizadas oito rodadas de negociações comerciais. Nas cinco primeiras reuniões (Genebra, 1947; Annecy, 1949; Torquay, 1950-1951; Genebra, 1955-1956; e Dillon, 1960-1961), buscou-se iniciar e instrumentalizar o processo de reduções e desagravos tarifários, sendo as discussões posteriormente ampliadas para outras áreas relevantes do comércio internacional.

Nas sexta e sétima reuniões, ocorridas em Kennedy (1964-1967) e Tóquio (1973-1979), além da questão tarifária, discutiu-se também medidas antidumping e medidas não tarifárias e cláusula de habilitação[97], respectivamente, sendo a Rodada Kennedy foi também marcada pela primeira participação da União Europeia, na qualidade de bloco econômico.

Na oitava reunião, a Rodada Uruguai (1986-1994), foram discutidas questões relativas a tarifas, agricultura, serviços, propriedade intelectual, medidas de investimento. Diante dessa multiplicidade de matérias objeto dos debates e discussões, verificou-se, também, a necessidade de se atualizar as regras e disciplinas do GATT-1847, culminando com a criação da OMC e de um novo conjunto de acordos multilaterais que formaram o corpo normativo da organização, adequados e aptos ao novo cenário internacional.

A OMC foi criada pelo Acordo de Marrakesh (1994), resultado da finalização da Rodada Uruguai de negociações comerciais (1986-1994). O acordo foi firmado em 1994, e passou a vigorar a partir de 1º de janeiro de 1995, sendo estruturado como um acordo-base (o acordo constitutivo da OMC), três anexos contendo acordos obrigatórios (multilaterais) e um anexo contendo acordos opcionais (plurilaterais).

Desde então, a OMC tem atuado como a principal instância reguladora do sistema multilateral de comércio. De acordo com BURRI (2017a, p. 71), a OMC representa o grau mais elevado de institucionalização da globalização econômica e representa um esforço para constitucionalizar a regulamentação do comércio, afastando-se de formas de governança mais antigas, baseadas na diplomacia, para

[97] A cláusula de habilitação estabelece exceção ao princípio da nação mais favorecida, possibilitando que os países desenvolvidos concedessem tratamento diferenciado e mais favorável aos países em desenvolvimento, sem reciprocidade, bem como que estes concedessem preferências entre si sem a necessidade de estendê-las aos países desenvolvidos.

princípios jurídicos e normas mais rigorosos. Para LEE (2018, p. 22), a OMC tem sido o acordo comercial mais importante e vinculativo desde 1995.

Em comparação ao GATT-1947, a OMC promoveu significativas modificações no sistema multilateral de comércio, destacando-se a incorporação dos produtos têxteis e agrícolas ao sistema; inclusão de regras sobre propriedade intelectual e investimento estrangeiros; adoção de um novo sistema de solução de controvérsias, com base na regra do consenso negativo[98]; adoção da regra do *single undertaking* (compromisso único)[99]; e revogação da *grandfather clause*[100].

Ao buscar o livre comércio, a abertura dos mercados e a diminuição do protecionismo, a OMC endossa uma série de princípios de não discriminação. Os princípios básicos do sistema multilateral de comércio estão estabelecidos nos arts. I, II e III do GATT-1994.

A cláusula da nação mais favorecida, prevista no art. I do GATT-1994, estabelece que todo e qualquer favorecimento alfandegário oferecido a um país-membro deve ser extensível aos demais. Objetiva, assim, garantir a não discriminação entre produtos similares originários de ou destinados a membros da OMC.

Desse modo, os países-membros são obrigados a estenderem, imediata e incondicionalmente, a todos os seus parceiros comerciais, qualquer concessão, benefício ou privilégio concedido a outro país-membro da OMC. Excepcionalmente, admite-se a concessão de benefícios por países desenvolvidos a países em desenvolvimento ou mútua outorga de benefícios por países em desenvolvimento e no caso dos acordos regionais de comércio enquadrados como união aduaneira ou zona de livre comércio.

O art. III do GATT-1994 estabelece a obrigação de não se aplicar a legislação interna de maneira a conferir proteção à produção nacional, de modo que os bens importados devem receber o mesmo tratamento concedido a produto equivalente de

---

[98] O sistema de solução de controvérsias do GATT-1947 seguia a regra do consenso positivo, ou seja, para que uma disputa fosse iniciada, um parecer técnico sobre a questão fosse aprovado e medidas retaliatórias fossem aprovadas, era necessária a aprovação da unanimidade dos países membros, inclusive do Estado supostamente violador das normas da OMC.

[99] Pela regra do *single undertaking*, à exceção dos acordos plurilaterais, constantes do anexo 4 do acordo constitutivo da OMC, que são opcionais, os demais acordos somente podem ser aceitos em bloco.

[100] A *grandfather clause* garantia às regulações nacionais anteriores ao advento do GATT-1947 uma imunidade às regras da parte II do acordo.

origem nacional. A regra do tratamento nacional, como é conhecida, visa garantir a não discriminação entre produtos nacionais e importados, em desfavor destes.

Pelo princípio da consolidação tarifária (art. II do GATT-1994), é vedada a aplicação de tarifas aduaneiras em montante superior à tarifa consolidada (valor máximo de alíquota do imposto de importação que cada país-membro se compromete a aplicar para determinados produtos) indicada na lista de concessões tarifárias.

Embora a OMC tenha herdado do GATT-1947 um conjunto de princípios que fundamentam a regulamentação multilateral do comércio, o fato é que o conjunto normativo atual é em grande parte o resultado das negociações da Rodada Uruguai.

Tais acordos são classificados em acordos multilaterais (Anexos 1A, 1B, 1C, 2 e 3), de adesão obrigatória, e acordos plurilaterais (Anexos 4A, 4B, 4C e 4D), de adesão opcional. No total, o marco jurídico da OMC compreende 30 acordos, além de compromissos específicos assumidos por determinados membros.

O Anexo 1 compreende “os três pilares do marco jurídico da OMC” (BURRI, 2017, p. 72): o Acordo Geral sobre Tarifas e Comércio (“GATT-1994”) (Anexo 1A), o Acordo Geral sobre o Comércio de Serviços (“GATS”) (Anexo 1B) e o Acordo sobre Aspectos dos Direitos de Propriedade Intelectual (“TRIPS”) (Anexo 1C).

O Anexo 3 trata do “Mecanismo de Exame de Políticas Comerciais”. Através da apreciação e avaliação coletiva e regular das políticas comerciais de cada país membro e de seu impacto sobre o funcionamento do sistema multilateral de comércio, o mecanismo de exame tem como objetivo contribuir para o melhor funcionamento do sistema multilateral de comércio.

Os acordos plurilaterais compreendem o Acordo sobre o Comércio de Aeronaves Civis (Anexo 4A), o Acordo sobre Compras Governamentais (Anexo 4B), o Acordo Internacional de Produtos Lácteos (Anexo 4C) e o Acordo Internacional sobre Carne Bovina (Anexo 4D), único que conta com a adesão do Brasil.

Embora não haja uma disposição específica no GATT-1994 sobre proteção de dados pessoais, privacidade ou questões relacionadas à economia digital, não se pode descartar a importância desse acordo para a economia digital, pois o desenvolvimento de um sistema de comunicação global com capacidade de tráfego e conectividade suficientes, bem como o comércio de toda a infraestrutura de TI

necessária, sustentáculos da economia digital, dependem necessariamente do cumprimento das regras do GATT-1994.

Em primeiro lugar, o GATT-1994 procurou liberalizar o comércio internacional proibindo, de modo geral, restrições quantitativas, instrumentos que limitam o valor ou o volume de importação de um determinado produto, podendo indicar também as quantidades que cada país pode importar individualmente.

Além disso, o GATT-1994 buscou reduzir e vincular as tarifas comerciais aplicadas pelos países membros, proibindo-os de aplicarem tarifas mais altas do que aquelas originalmente acordadas (princípio da consolidação de tarifas). Por força da aplicação do princípio da nação mais favorecida, previsto no art. I do GATT-1994, qualquer vantagem, favor, imunidade ou privilégio concedido por um país membro em relação a um produto originário de ou destinado a qualquer outro país, será imediata e incondicionalmente estendido ao produtor similar, originário do território de cada um dos outros membros ou a eles destinado.

Já o GATS se aplica às medidas adotadas pelos países membros que afetem a prestação de serviços, incluindo a sua produção, distribuição, comercialização, venda e entrega.

A contribuição do GATS para o comércio mundial de serviços baseia-se em três pilares principais: assegurar maior transparência e previsibilidade de regras e regulamentações relevantes; prover uma estrutura comum de disciplinas para transações internacionais; e promover progressiva liberalização através de sucessivas rodadas de negociações.

Ao reconhecer a importância crescente do comércio de serviços para o crescimento e desenvolvimento da economia mundial, o GATS procurou estabelecer um quadro de princípios e regras aplicáveis ao comércio de serviços, com o objetivo de possibilitar sua expansão e liberalização progressiva, bem como de facilitar a participação crescente dos países em desenvolvimento no comércio de serviços.

O art. I estipula que o GATS se aplica às medidas dos países-membros que afetam o comércio de serviços, assim considerado “qualquer serviço em qualquer setor, exceto aqueles prestados no exercício da autoridade governamental”, ou seja, “qualquer serviço que não seja prestado em bases comerciais, nem em competição com um ou mais prestadores de serviço”.

Neste contexto, o GATS abrange quaisquer medidas, sejam em forma de lei, regulamento, regra, procedimento, decisão judicial ou administrativa ou sob qualquer outra forma, referentes a compra, pagamento ou utilização de um serviço; o acesso e a utilização, por ocasião da prestação de um serviço, de serviços que o membro exija sejam oferecidos ao público em geral; e a presença, inclusive a presença comercial, de pessoas de um membro para a prestação de um serviço no território de outro membro.

A definição de comércio de serviços sob o GATS tem quatro vertentes, dependendo da presença territorial do fornecedor e do consumidor no momento da prestação do serviço. De acordo com o art. I (2), o GATS compreende os seguintes modos de prestação de serviços:

a) fornecidos do território de um membro ao território de qualquer outro membro (Modo 1 - comércio transfronteiriço);
b) fornecidos no território de um membro aos consumidores de serviços de qualquer outro membro (Modo 2 – consumo no exterior);
c) fornecidos pelo prestador de serviços de um membro, por intermédio da presença comercial no território de qualquer outro membro (Modo 3 – presença comercial);
d) fornecidos pelo prestador de serviços de um membro por intermédio da presença de pessoas naturais de um membro no território de qualquer outro membro (Modo 4 – presença de pessoas naturais).

Com fins de sistematizar seus compromissos, os Estados Membros da OMC utilizam a Classificação Central de Produtos Básicos (CPC) das Nações Unidas[101], que lista doze categorias de setores de serviços principais: serviços de empresas (incluindo serviços de informática e conexos e de pesquisa e desenvolvimento); serviços de comunicação; serviços de construção e relacionados à engenharia; serviços de distribuição; serviços educacionais; serviços de meio ambiente; serviços financeiros; serviços de saúde e sociais (exceto os médicos, dentários e veterinários,

[101] Esta classificação é informalmente referida como “W120”, pois é este o símbolo do documento oficial da OMC que serve como sua base.

que são classificados como serviços de empresas); serviços de turismo e relacionados; serviços de diversão, cultural e esportivos; serviços de transportes; e outros serviços não incluídos anteriormente. Esses setores são subdivididos outros 160 subsetores.

Embora esse sistema não esteja atualizado com os novos desenvolvimentos tecnológicos (MITCHELL e HEPBURN, 2017, p. 198), entre as categorias mais amplas, serviços de empresas, de comunicação e financeiros são os mais relevantes para a economia digital e, em menor grau, os serviços educacionais e de turismo. Em serviços de empresas, destaca-se as subcategorias serviços de pesquisa e desenvolvimento e serviços de informática e conexos, especialmente os serviços de processamento de dados e de base de dados; em serviços de comunicação, as subcategorias de serviços de telecomunicações (incluindo serviços de transmissão de pacotes de dados; serviços de transmissão de dados com computação de circuitos; extração de informação em linha e de bases de dados; intercâmbio eletrônico de dados; e processamento de dados e informações *online*) e audiovisuais são os mais relevantes para a economia digital. Em relação aos serviços financeiros, destaca-se a subcategoria serviços bancários e outros serviços financeiros, que inclui o provimento e a transferência de informações financeiras, processamento de dados financeiros e programas de computador de outros provedores de serviços financeiros.

No âmbito do GATS, as obrigações assumidas pelos países-membros podem ser divididas em gerais e específicas. Aquelas, relativas ao tratamento da nação mais favorecida e à transparência, aplicam-se automaticamente a todos os países e setores de serviços; estas, relativas ao acesso a mercados e tratamento nacional, são negociadas individualmente por cada país-membro para setores de serviços e modos de prestação determinados.

Assim, os compromissos específicos somente se aplicam aos setores de serviços expressamente previstos por cada país-membro em sua lista de compromissos, e novos serviços não estão automaticamente cobertos pelo GATS, o que restringe o efeito liberalizante originalmente pretendido pelo acordo (WEBER, 2012, p. 28)

A principal obrigação geral está prevista no art. II do GATS, relativa à cláusula da nação mais favorecida. Por esse princípio, como visto, cada país-membro deve

conceder imediata e incondicionalmente aos serviços e prestadores de serviços de qualquer outro membro, tratamento não menos favorável do aquele concedido a serviços e prestadores de serviços similares de qualquer outro país.

Ao contrário do GATT-1994, no entanto, que não admite exceções ao tratamento da nação mais favorecida, o GATS autoriza a inaplicabilidade desse princípio a determinadas medidas, desde que esteja listada e satisfaça as condições do Anexo sobre Isenções das Obrigações do Artigo II.

Os Estados Membros também devem comunicar à OMC a existência de normas internas ou outros acordos internacionais de que sejam parte que possam afetar a aplicação do GATS. A obrigação de transparência permanece importante, seja porque os marcos regulatórios nacionais permanecem em constante evolução, seja porque há vários países ainda em negociação para ingressar na OMC, cujas normas internas deverão ser prontamente revistas para se adequarem aos compromissos assumidos perante a organização e demais países-membros.

Pelo compromisso de acesso a mercados, previsto no art. XVI do GATS, os países-membros devem garantir aos prestadores de serviços e serviços dos demais membros um tratamento não menos favorável do que o previsto sob os termos, limitações e condições acordadas e especificadas em sua lista de compromissos. O objetivo do compromisso de acesso a mercados é impedir a imposição de restrições quantitativas ao comércio de serviços.

As hipóteses de limitação ao compromisso de acesso a mercados estão taxativamente previstas no art. XVI(2), e se referem ao número de prestadores de serviços, ao valor dos ativos ou das transações realizadas, ao número de operações de serviços ou quantidade de serviços produzidos, ao número de empregados, à estrutura societária da operação, e à participação de capital estrangeiro.

O outro compromisso previsto no GATS é o do tratamento nacional (art. XVII), de conteúdo semelhante àquele previsto no âmbito do GATT, ou seja, os países-membros devem outorgar aos serviços e prestadores de serviços de outros membros um tratamento não menos favorável do que aquele dispensado aos serviços e prestadores de serviços similares nacionais. O compromisso do tratamento nacional busca afastar a imposição de restrições qualitativas ao comércio de serviços.

Assim como a obrigação de acesso a mercados, o compromisso do tratamento nacional também pode ser limitado, mas de forma mais ampla, sendo possível aos países-membros estabelecerem quaisquer condições e qualificações em suas listas de compromisso.

O GATS estabelece, ainda, as chamadas exceções gerais, previstas no seu art. XIV. Elas permitem que os países-membros da OMC adotem medidas que, de outra forma, violariam as obrigações e os compromissos assumidos, sob a condição de que essas medidas não sejam restrições disfarçadas ao comércio.

Embora o art. XIV enumere diferentes fundamentos, como possíveis justificativas, como a proteção da vida ou saúde humana, animal ou vegetal, no que se refere ao presente estudo, destaca-se aquelas relacionadas à proteção da moral e manutenção da ordem pública e aquelas necessárias à garantia a observância das leis e regulamentos, dentre os quais aquelas com relação à proteção da privacidade de indivíduos em relação ao processamento e à disseminação de dados pessoais e à proteção da confidencialidade de registros e contas pessoais.

2.5.3.2. Os acordos da OMC e as novas tecnologias

Os Anexos do GATS sobre Serviços Financeiros e Telecomunicações tratam da transferência de dados. O Artigo 8º do Entendimento sobre Compromissos em Serviços Financeiros estabelece que:

> Nenhum Membro deve adotar medidas que impeçam a transferência de informações ou o processamento de informações financeiras, incluindo transferências de dados por meios eletrônicos, ou que, sujeito a regras de importação compatíveis com acordos internacionais, impeçam a transferência de equipamentos, quando tais transferências de informações, processamento de informações financeiras ou transferências de equipamentos sejam necessárias para a condução dos negócios comuns de um fornecedor de serviços financeiros. Nada neste parágrafo restringe o direito de um Membro de proteger dados pessoais, privacidade pessoal e a confidencialidade de registros e contas individuais, desde que esse direito não seja usado para contornar as disposições do Contrato[102].

[102] Tradução livre do original: “No Member shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this paragraph restricts the right of a Member to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of the Agreement.”

Já o Anexo sobre Telecomunicações estabelece que os Estados Membros devem assegurar aos prestadores de serviços de qualquer outro Estado Membro o acesso às e a utilização das redes públicas de transporte de telecomunicações e serviços para a movimentação de informações dentro e através das fronteiras, inclusive para a comunicação intra-empresa de tais prestadores de serviços e para o acesso a informações contidas em bancos de dados ou armazenadas de outra forma legível por máquina no território de qualquer Estado Membro.

No entanto, o fato é que os acordos da OMC foram negociados durante a Rodada Uruguai de negociações, realizada entre 1986 e 1994, quando a internet comercial ainda estava em seus primeiros estágios de desenvolvimento, situação completamente diferente da vivida atualmente, marcada pela digitalização onipresente e aprofundamento de redes interconectadas, que mudaram o volume, a intensidade, a potência e a natureza dos fluxos de dados (BURRI, 2017a, p. 69)

Embora a Internet tivesse começado na mente dos cientistas da computação no início da década de 1960, uma rede de comunicações por computador tivesse sido formada em 1969, e comunidades dispersas de computação reunindo cientistas e hackers tivessem brotado desde o final da década de 1970, para a maioria das pessoas, para os empresários e para a sociedade em geral, foi em 1995, já privatizada e dotada de uma arquitetura técnica aberta, permitindo a interconexão de todas as redes de computadores em qualquer lugar do mundo, que ela nasceu.

Por essa razão, os acordos da OMC reconhecem a importância dos fluxos internacionais de dados de forma bastante limitada (MITCHELL a MISHRA, 2018, p. 1091). À exceção de disposições esparsas constantes do Anexo sobre Serviços Financeiros e Anexo sobre Telecomunicações do GATS, não há nos acordos da OMC dispositivos que tratem especificamente do comércio eletrônico e do fluxo internacional de dados.

Por exemplo, o Anexo sobre Telecomunicações do GATS reconhece a importância dos fluxos internacionais de dados, ao mesmo tempo em que reafirma a importância da privacidade e proteção de dados. Da mesma forma, no Anexo sobre Serviços Financeiros, os Estados Membros concordam em não impedir transferências de informações ou o processamento de informações financeiras, incluindo transferências de dados por meios eletrônicos.

No entanto, as regras acima somente se aplicam a serviços que se enquadram no escopo dos setores financeiro e de telecomunicações. Os fluxos internacionais de dados relativos a serviços digitais em outros setores não são explicitamente protegidos.

Assim, embora o aspecto cronológico explique a ausência de um tratamento específico sobre essas matérias nos acordos da OMC, o fato é que, passados quase 25 anos desde o início da vigência da OMC (01/01/1995), a despeito da criação do *WTO Work Programme on Electronic Commerce* [103] e de poucas atualizações normativas, como o Acordo sobre Tecnologia da Informação (ITA) [104] e o Quarto Protocolo sobre Serviços de Telecomunicação Básica, as regras da OMC não acompanharam a rápida evolução da internet, tornando-se ineficazes para enfrentar os desafios contemporâneos do comércio digital e facilitar a liberalização do setor digital (MITCHELL a MISHRA, 2018, p. 1088).

Enquanto os fluxos de dados se limitavam a poucas transmissões entre empresas ou governos, agora, os dados podem ser transferidos globalmente; processados de forma simultânea em vários locais; armazenados em qualquer local do planeta; recombinados instantaneamente (BURRI, 2017b, p. 69 e 70).

Nesse contexto, diversos problemas surgem do descompasso entre os acordos da OMC e a realidade atual da economia digital, criando uma situação de insegurança jurídica. Alguns se relacionam com classificações antigas (pré internet) de bens, serviços e setores, nas quais esses compromissos se baseavam e que estão

---

103 Na Segunda Conferência Ministerial, em maio de 1998, os ministros, reconhecendo que o comércio eletrônico global estava crescendo e criando novas oportunidades para o comércio, adotaram a Declaração sobre Comércio Eletrônico Global. Isso exigia o estabelecimento de um programa de trabalho sobre comércio eletrônico, adotado em setembro de 1998. As revisões periódicas do programa são conduzidas pelo Conselho Geral com base em relatórios dos órgãos da OMC responsáveis pela implementação do programa. Os ministros também consideram regularmente o programa nas conferências ministeriais da OMC.

104 O ITA foi adotado durante a Conferência Ministerial de Singapura, realizada em 1996. Seus objetivos são alcançar a liberdade máxima do comércio mundial de produtos de tecnologia da informação; incentivar o desenvolvimento tecnológico contínuo do setor de tecnologia da informação em nível mundial; e aprimorar as oportunidades de acesso ao mercado para informações. produtos de tecnologia. Para esse efeito, os signatários da ITA se comprometeram a fornecer tarifas zero para produtos de TI selecionados, como computadores, semicondutores, equipamentos de fabricação de semicondutores, aparelhos de telecomunicações, mídia de armazenamento de dados e software. O ITA não é um acordo multilateral, mas plurilateral, o que significa que apenas vincula as partes signatárias. No entanto, diferentemente de outros acordos plurilaterais, o ITA é acordo aberto, de modo que seus benefícios podem ser invocados todos os membros da OMC, incluindo aqueles que não fazem parte do acordo.

cada vez mais desconectados das práticas comerciais. Outros dizem respeito à maneira como as regras da OMC, em particular as disposições do GATS, foram elaboradas, permitindo que os países-membros adaptem seus compromissos.

Em primeiro lugar, a aplicação de certas obrigações legais sob o GATS (como tratamento nacional e acesso ao mercado) depende do escopo dos compromissos assumidos pelos países-membros (MITCHELL e MISHRA, 2018, p. 1089). Em outras palavras, os Estados Membros da OMC desfrutam de considerável autonomia para determinar em que medida estão dispostos a abrir seus mercados a empresas estrangeiras.

Possíveis dificuldades surgem na classificação das transferências de dados sob os amplos conceitos de bens e serviços na OMC. A questão da classificação de produtos com uso intensivo de dados não é meramente uma questão de semântica, porque as regras aplicáveis a um produto dependem de sua classificação. Se o modo de entrega de um produto digital é através de uma cópia física, aplica-se o GATT, que depende do fato de que o produto é físico em substância e seu modo de entrega exige que o produto ultrapasse fisicamente as fronteiras nacionais. No entanto, se o mesmo produto também for distribuído eletronicamente, aplica-se o GATS, independentemente do modo de entrega.

Outra questão relevante diz respeito à classificação dos serviços de acordo com os modos de prestação, isto é, se a prestação de serviços com uso intensivo de dados caracteriza a prestação de serviços transfronteiriço (Modo 1 do GATS) ou consumo de um serviço no exterior (Modo 2 do GATS).

A classificação simultânea nos dois modos pode criar dificuldades na identificação dos compromissos relevantes do país-membro quando os compromissos para o setor relevante diferem entre os dois modos (MITCHELL e HEPBURN, 2017, p. 197).

Conceitualmente, durante o fluxo de dados e o comércio de serviços com uso intensivo de dados, nem o comprador nem o vendedor cruzam as fronteiras do estado, pelo menos no sentido físico. Por essa razão, a visão majoritária é de que os fluxos de dados constituem um problema de transação no Modo 1 (SEN, 2018, p. 10).

No entanto, para determinados produtos, como serviços financeiros, é possível afirmar que o consumo do serviço ocorrer no exterior, uma vez que o serviço

não está sendo fornecido no servidor do dispositivo do consumidor, mas no servidor do dispositivo do vendedor.

Nesses casos, os dados podem ser hospedados em um país estrangeiro onde os servidores do vendedor estão localizados e, quando o consumidor deseja acessar os dados, o consumo virtual no exterior é ativado pelo fluxo de dados. Esses casos seriam uma hipótese de transação do Modo 2.

Além disso, embora a Classificação Central de Produtos Básicos (CPC) das Nações Unidas forneça um ponto de referência, essa classificação tem quase três décadas e não representa adequadamente os setores de negócios da economia digital (MITCHELL e MISHRA, 2018, p. 1089-1090).

No julgamento do caso *US-Gambling*, o Órgão de Apelação da OMC entendeu que os setores e subsetores de serviços são mutuamente exclusivos. Essa exclusividade se torna problemática à luz dos novos modelos de negócios da economia digital, que compreendem plataformas digitais que interligam vários serviços e produtos com uso intensivo de dados, uma vez que esses serviços costumam ter vários usos finais. Consequentemente, esses serviços podem ser classificados em várias categorias, a exemplo da subcategoria de “processamento de dados”, que aparece duas vezes na classificação W/120, uma vez em “serviços de informática e serviços correlatos” e outra em “serviços de telecomunicações”.

Além do problema de sobreposição, as categorias de classificação W/120 também são insuficientes para acomodar novos serviços que surgiram desde a elaboração e adoção do sistema e que não se enquadram diretamente em nenhuma das categorias atualmente disponíveis. Como muitos desses novos produtos e serviços eram inimagináveis durante o início do GATS, há insegurança jurídica sobre se esses produtos se encaixam em setores especificados no W/120 ou se constituem setores completamente novos.

A despeito disso, TUTHILL (2016, apud MITCHELL e BURRI, 2016) argumenta que as disposições existentes no GATS são suficientes para endereçar as principais questões relacionadas ao fluxo internacional de dados e os impactos de sua restrição para o comércio internacional.

Em primeiro lugar, ele considera que um requisito de localização constitui um requisito de presença comercial sob o GATS, de modo que, se os países-membros

da OMC não tiverem inscrito nenhuma limitação no fornecimento de serviços do Modo 3 nos setores relevantes, haveria uma violação ao compromisso do tratamento nacional.

Além disso, ele argumenta que os requisitos de localização podem ser considerados requisitos de conteúdo local (ou seja, usando servidores e recursos locais). Como a maioria dos países-membros da OMC não listou limitações para o conteúdo local em seu cronograma de compromissos para a maioria dos serviços de tecnologia da informação e comunicação, essas restrições violariam o GATS.

Por outro lado, LEE-MAKIYAMA (2013, apud MITCHELL e BURRI, 2016) defende que, como o GATS se destinava a liberalizar as comunicações de voz (por exemplo, no Anexo sobre Telecomunicações), em vez de transferências de dados, o acordo é ineficaz no contexto da Internet.

Para ele, as obrigações legais sobre fluxos internacionais de dados estão sujeitas aos compromissos específicos assumidos pelos países-membros em vários setores, incluindo o setor de telecomunicações e serviços de informática e serviços relacionados.

Tendo em conta que a classificação dos serviços digitais modernos não é clara, a falta de comprometimento horizontal nos fluxos internacionais de dados no âmbito do GATS, juntamente com a complexidade na classificação de serviços digitais, torna incerta a natureza dos compromissos legais assumidos.

2.6. Iniciativas regionais

2.6.1. União Europeia

Nos termos do Artigo 16 do Tratado sobre o Funcionamento da União Europeia, compete ao Parlamento Europeu e ao Conselho estabelecerem as normas relativas ao tratamento de dados pessoais pelas instituições, órgãos e organismos da União Europeia, bem como pelos Estados-Membros no exercício de atividades relativas à aplicação do Direito Europeu, e à livre circulação desses dados.

A Diretiva Europeia de Proteção de Dados (Diretiva 95/46/CE) foi adotada em 1995, como resultado dos esforços da Comissão Europeia para a concretização dos objetivos do mercado único. A Comissão Europeia estava preocupada que a

existência de diferentes padrões de proteção de dados entre os Estados Membros pudesse inibir o livro fluxo de dados dentro da União Europeia. De acordo com SCHWARTZ (2013, p. 1972):

> Na UE, os anos 90 foram um período de maior atividade econômica e de maior demanda por informações pessoais. Na ausência de normas em toda a UE, a transferência de dados na UE tinha potencial para minar os esforços, desde a década de 1970, de cada um dos estados membros para proteger as informações pessoais de seus cidadãos[105].

Os principais objetivos da Diretiva eram facilitar o livre fluxo de dados dentro da União Europeia e assegurar o mesmo nível de proteção em todos os Estados-Membros. De acordo com SCHWARTZ (2013, p. 1972), "A abordagem regulatória resultante combinou a liberalização econômica do comércio envolvendo dados pessoais com políticas harmonizadas para proteger as liberdades civis"[106]. Esses objetivos estão refletidos nos itens n° 7, 8 e 9 do preâmbulo da Diretiva:

> (7) Considerando que as diferenças entre os Estados-membros quanto ao nível de proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada, no domínio do tratamento de dados pessoais, podem impedir a transmissão desses dados do território de um Estado-membro para o de outro Estado-membro; que estas diferenças podem, por conseguinte, constituir um obstáculo ao exercício de uma série de atividades económicas à escala comunitária, falsear a concorrência e entravar o exercício pelas administrações das funções que lhes incumbem nos termos do direito comunitário; que esta diferença de níveis de proteção resulta da disparidade das disposições legislativas, regulamentares e administrativas nacionais;
>
> (8) Considerando que, para eliminar os obstáculos à circulação de dados pessoais, o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento destes dados deve ser equivalente em todos os Estados-membros; que a realização deste objetivo, fundamental para o mercado interno, não pode ser assegurada unicamente pelos Estados-membros, tendo especialmente em conta a dimensão das divergências que se verificam atualmente a nível das legislações nacionais aplicáveis na matéria e a necessidade do coordenar as legislações dos Estados-membros para assegurar que a circulação transfronteiras de dados pessoais seja regulada de forma coerente e em conformidade com o objetivo do mercado interno nos termos do artigo 7º A do Tratado; que é portanto necessária uma ação comunitária com vista à aproximação das legislações;
>
> (9) Considerando que, devido à proteção equivalente resultante da aproximação das legislações nacionais, os Estados-membros deixarão de

[105] Tradução livre do original em inglês: "Within the EU, the 1990s were a period of increased economic activity and of heightened demands for personal information. In the absence of EU-wide standards, data transfer within the EU had potential to undermine efforts, darting back to the 1970s, of individual member states to protect the personal information of their citizens".

[106] Tradução livre do original em inglês: "The resulting regulatory approach combined economic liberalization of trade involving personal data with harmonized policies to protect civil liberties".

> poder levantar obstáculos à livre circulação entre si de dados pessoais por razões de proteção dos direitos e liberdades das pessoas, nomeadamente do direito à vida privada; que é deixada aos Estadas-membros uma margem de manobra que, no contexto da aplicação da diretiva, poderá ser utilizada pelos parceiros económicos e sociais; que os Estados-membros poderão, pois, especificar na sua legislação nacional as condições gerais de licitude do tratamento de dados; que, ao fazê-lo, os Estados-membros se esforçarão por melhorar a proteção atualmente assegurada na respectiva legislação nacional; que, nos limites dessa margem de manobra e em conformidade com o direito comunitário, poderão verificar-se disparidades na aplicação da diretiva, o que poderá refletir-se na circulação de dados quer no interior de um Estado-membro, quer na Comunidade.

Interessante observar que, embora o uso comercial da internet ainda estivesse dando os primeiros passos naquela época, já havia a clara percepção da importância da transferência internacional de dados na promoção do desenvolvimento econômico e social:

> (5) Considerando que a integração económica e social resultante do estabelecimento e funcionamento do mercado interno nos termos do artigo 7º A do Tratado irá necessariamente provocar um aumento sensível dos fluxos transfronteiras de dados pessoais entre todos os intervenientes, privados ou públicos, na vida económica e social dos Estados-membros; que o intercâmbio de dados pessoais entre empresas estabelecidas em diferentes Estados-membros tende a intensificar-se; que as administrações dos Estados-membros são chamadas, por força do direito comunitário, a colaborar e a trocar entre si dados pessoais a fim de poderem desempenhar as suas atribuições ou executar tarefas por conta de uma administração de outro Estado-membro, no âmbito do espaço sem fronteiras internas que o mercado interno constitui;
>
> (6) Considerando, além disso, que o reforço da cooperação científica bem como a introdução coordenada de novas redes de telecomunicações na Comunidade exigem e facilitam a circulação transfronteiras de dados pessoais;
>
> (56) Considerando que os fluxos transfronteiras de dados pessoais são necessários ao desenvolvimento do comércio internacional; que a proteção das pessoas garantida na Comunidade pela presente diretiva não obsta às transferências de dados pessoais para países terceiros que assegurem um nível de proteção adequado; que o carácter adequado do nível de proteção oferecido por um país terceiro deve ser apreciado em função de todas as circunstâncias associadas à transferência ou a uma categoria de transferências;

O impacto da Diretiva foi relevante, seja por ter moldado a forma de inúmeras leis, dentre e fora da União Europeia, seja por ter contribuído para o desenvolvimento

de um modelo europeu de proteção de dados, tendo estabelecido o padrão em matéria de transferência internacional de dados durante duas décadas.

Desde 25 de maio de 2018, o Regulamento Geral sobre Proteção de Dados da União Europeia (Regulamento 2016/679) ("GDPR"), que estabelece as regras relativas ao tratamento, por uma pessoa, uma empresa ou uma organização, de dados pessoais relativos a pessoas na União Europeia, passou a ser aplicado automaticamente nos Estados-Membros, substituindo a legislação anterior sobre a matéria (Diretiva 95/46/CE).

Para SCHWARTZ e PEIFER (2017, p. 128), "(...) a decisão de substituir a diretiva relativa à proteção de dados por um regulamento demonstra a importância crescente da privacidade das informações da UE como uma questão estatutária"[107]. Nesse mesmo sentido, MELTZER e MATTOO (2017, p. 772) consideram que "O GDPR, adotado pela UE em maio de 2018 para substituir a diretiva anterior de proteção de dados, reflete a importância da privacidade como direito humano e seu significado na UE"[108].

É que, ao contrário dos regulamentos, de aplicação obrigatória, automática e imediata pelos Estados-Membros, as diretivas dependem da promulgação de leis nacionais que reflitam suas regras e princípios. Além da evidente multiplicação de diferentes leis sobre a mesma matéria, que atrai o problema da sobreposição normativa e do conflito de leis (no tempo e no espaço), a ausência de força vinculante enfraqueceu a aplicação da Diretiva 95/46/CE, criando distorções, inclusive, do ponto de vista concorrencial, o que justificou a sua substituição pelo GDPR, conforme expressamente refletido no item n° 9 do seu preâmbulo:

> Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrônica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas

[107] Tradução livre do original em inglês: "(...) the decision to replace the Data Protection Directive with a Regulation demonstrates the rising significance of EU information privacy as a statutory matter".
[108] Tradução livre do original em inglês: "The GDPR, adopted by the EU in May 2018 to replace the earlier Data Protection Directive, reflects the importance of privacy as human right and its significance in the EU".

> a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE.

Ao analisar as razões que levaram à elaboração de um novo marco regulatório de proteção da privacidade e dos dados pessoais na União Europeia, SCHWARTZ (2013, p. 1993) aponta que:

> Por exemplo, os Estados-Membros estavam interpretando as regras de consentimento de maneira diferente, e a concessão pela Diretiva de "espaço de manobra em determinadas áreas" e seus Estados-Membros permitindo que emitissem "regras específicas para situações específicas" criaram "custos adicionais e encargos administrativos" para partes interessadas privadas. Devido a esta falta de uniformidade nos termos da diretiva, era necessário um regulamento para criar segurança jurídica no mercado interno e garantir um papel contínuo para a UE na promoção de altos padrões de proteção de dados em todo o mundo[109].

Nesse sentido, a Comissão Europeia ressalta a importância do GDPR, que "(...) estabelecerá um conjunto único de regras pan-europeias que tornará mais simples e barato para as empresas fazerem negócios na UE e garantirá que os direitos das pessoas sejam protegidos de maneira mais eficaz em todo o continente"[110].

O GDPR tem como objetivo principal "contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união econômica, para o progresso econômico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares" (item n° 2 do preâmbulo), bem como assegurar **(a)** um nível coerente de proteção e evitar que eventuais divergências constituam um obstáculo à livre circulação de dados pessoais no mercado interno europeu; **(b)** segurança jurídica e transparência às empresas; **(c)** os mesmos direitos a todos os cidadãos europeus, bem como obrigações e

[109] Tradução livre do original em inglês "For example, member states were interpreting the rules for consent differently, and the Directive's grant of 'room for manoeuvre in certain areas' and its permitting member states to issue 'particular rules for specific situations 'had created additional cost[s] and administrative burden[s]' for private stakeholders. Due to this absence of uniformity under the Directive, a regulation was needed to create legal certainty within the internal market and to assure a continuing role for the EU 'in promoting high data protections standards worldwide

[110] Tradução livre do original em inglês: "(...) will establish one single pan-European set of rules that will make it simpler and cheaper for companies to do business in the EU, and will ensure that the rights of individuals are more effectively protected across de continent".

responsabilidades iguais aos agentes tratamento dos dados; **(d)** o controle coerente do tratamento dos dados pessoais, a aplicação de sanções equivalentes em todos os Estados-Membros e uma cooperação efetiva entre as autoridades nacionais (item n° 13 do preâmbulo).

O GDPR reconhece que a circulação de dados pessoais, com origem em ou destino a países não pertencentes à União Europeia ou a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais. Para SCHWARTZ e PEIFER (2017, p. 130), "[T]ambém há um reconhecimento aqui do valor monetário dos fluxos internacionais de informação. A UE tem um interesse de longa data na liberalização econômica do comércio e no acesso à economia global da informação"[111].

Além disso, o GDPR não prejudica os acordos internacionais celebrados entre a União Europeia e países terceiros que regulem a transferência de dados pessoais, incluindo as garantias adequadas em benefício dos titulares dos dados. Nos termos do Artigo 96º, "Os acordos internacionais celebrados pelos Estados Membros (...) que impliquem a transferência de dados pessoais para países terceiros ou organizações internacionais e que sejam conformes com o direito da União (...) permanecem em vigor até serem alterados, substituídos ou revogados".

Embora a arquitetura do novo regime de transferências internacionais seja semelhante à da Diretiva 95/46/CE, a reforma simplifica e amplia o uso de mecanismos existentes e introduz novas ferramentas para transferências internacionais de dados.

Nos termos do GDPR, os dados pessoais somente podem ser transferidos para fora da União Europeia se determinadas condições específicas estiverem preenchidas. A principal delas é a constatação pela Comissão Europeia de que países terceiros receptores dos dados pessoais fornecem um nível adequado de proteção. Na ausência de uma decisão de adequação, o GDPR oferece um conjunto de mecanismos para a transferência internacional de dados: cláusulas contratuais padrão, regras corporativas vinculantes, mecanismo de certificação, códigos de conduta e as chamadas derrogações.

---

[111] Tradução livre do original em inglês: "There is also a recognition here of the monetary value of international flows of information. The EU has a longstanding interest in economic liberalization of trade and in access to the global information economy".

O principal objetivo dessas normas de controle de transferência de dados é garantir que os dados pessoais de cidadãos europeus recebam o mesmo nível de proteção conferido pelo GDPR fora do território europeu, conforme expressamente previsto no item nº 101 do preâmbulo:

> (101) A circulação de dados pessoais, com origem e destino quer a países não pertencentes à União quer a organizações internacionais, é necessária ao desenvolvimento do comércio e da cooperação internacionais. O aumento dessa circulação criou novos desafios e novas preocupações em relação à proteção dos dados pessoais. Todavia, quando os dados pessoais são transferidos da União para responsáveis pelo tratamento, para subcontratantes ou para outros destinatários em países terceiros ou para organizações internacionais, o nível de proteção das pessoas singulares assegurado na União pelo presente regulamento deverá continuar a ser garantido, inclusive nos casos de posterior transferência de dados pessoais do país terceiro ou da organização internacional em causa para responsáveis pelo tratamento, subcontratantes desse país terceiro ou de outro, ou para uma organização internacional. Em todo o caso, as transferências para países terceiros e organizações internacionais só podem ser efetuadas no pleno respeito pelo presente regulamento. Só poderão ser realizadas transferências se, sob reserva das demais disposições do presente regulamento, as condições constantes das disposições do presente regulamento relativas a transferências de dados pessoais para países terceiros e organizações internacionais forem cumpridas pelo responsável pelo tratamento ou subcontratante.

Nesse sentido, de acordo com o princípio geral das transferências, previsto no Artigo 44º do GDPR, “qualquer transferência de dados pessoais (...) só é realizada se, sem prejuízo das outras disposições do presente regulamento, as condições estabelecidas no presente capítulo forem respeitadas (...)”.

O GDPR autoriza a transferência de dados pessoais para um país terceiro ou uma organização internacional sempre que houver uma decisão no sentido de que o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado. Trata-se das chamadas “transferência com base numa decisão de adequação”. Essas transferências não exigem uma autorização específica, de modo que, enquanto vigorar a decisão de adequação, poderá haver o livro fluxo de dados entre os Estados-Membros e países terceiros ou organizações internacionais.

Ao concluir que a ordem jurídica do país ou organização dispõe de um nível adequado de proteção, tal decisão reconhece que esse sistema se aproxima daquele vigente na União Europeia. Daí resulta que esses fluxos de dados serão equiparados

às transferências realizadas no âmbito da União Europeia, permitindo um acesso privilegiado ao mercado único europeu.

Em determinadas situações, no entanto, em vez de se optar por uma abordagem que englobe todo o país ou organização, pode ser mais adequado recorrer a outras opções, tais como uma decisão de adequação parcial ou específica para um determinado setor.

O efeito de tal decisão (ampla ou parcial) é que os dados pessoais podem ser transferidos da União Europeia (e da Noruega, Liechtenstein e Islândia) para outros países (fora da Área Econômica Europeia), sem necessidade de mais nenhuma salvaguarda. Em outras palavras, tais transferências serão equiparadas àquelas realizadas no interior da União Europeia.

Compete à Comissão Europeia decidir se determinado país ou organização internacional oferecem um nível adequado de proteção de dados, garantindo, assim, a segurança jurídica e a uniformidade ao nível da União Europeia.

Nas suas decisões de adequação, a Comissão deverá prever um procedimento de avaliação periódica, no mínimo de quatro em quatro anos, que deverá ter em conta todos os desenvolvimentos pertinentes no país terceiro ou na organização internacional. Caso se verifique que o país terceiro ou a organização internacional deixou de assegurar um nível de proteção adequado, a Comissão poderá, na medida do necessário, revogar, alterar ou suspender a decisão de adequação. Da mesma forma, a qualquer momento, o Parlamento Europeu e o Conselho podem solicitar à Comissão que mantenha, altere ou revogue a decisão de adequação com o fundamento de que o seu ato excede as competências de execução previstas no regulamento.

O GDPR elenca os fatores de risco que devem ser considerados pela Comissão Europeia ao avaliar o nível de adequação dos regimes de privacidade dos outros países. Nos termos do Artigo 45(2), do GDPR, ao avaliar a adequação do nível de proteção, a Comissão Europeia deverá levar em conta os seguintes elementos:

a) o primado do Estado de Direito, o respeito pelos direitos humanos e liberdades fundamentais, a legislação pertinente em vigor, tanto a geral como a setorial, especialmente em matéria de segurança pública, defesa, segurança nacional

e direito penal, e relativa ao acesso das autoridades públicas a dados pessoais, bem como a aplicação dessa legislação e das regras de proteção de dados, das regras profissionais e das medidas de segurança, incluindo as regras para a transferência posterior de dados pessoais para outro país ou organização internacional, que são cumpridas nesse país ou por essa organização internacional, e a jurisprudência, bem como os direitos dos titulares dos dados efetivos e oponíveis, e vias de recurso administrativo e judicial para os titulares de dados cujos dados pessoais sejam objeto de transferência;

b) a existência e o efetivo funcionamento de uma ou mais autoridades de controle independentes no país 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 controle dos Estados-Membros; e

c) os compromissos internacionais assumidos pelo país ou pela organização internacional, ou outras obrigações decorrentes de convenções ou instrumentos juridicamente vinculativos, bem como da sua participação em sistemas multilaterais ou regionais, em especial em relação à proteção de dados pessoais.

No julgamento do caso *Schrems v. Data Protection Commissionar*, ainda sob a vigência da Diretiva, o TJUE se manifestou no sentido de que se considera "adequado" o regime de privacidade "essencialmente equivalente" ao da União Europeia:

> É verdade que o termo "adequado" que figura no artigo 25º, nº 6, da Diretiva 95/46 implica que não se pode exigir que um país terceiro assegure um nível de proteção idêntico ao garantido na ordem jurídica da União. Porém, como o advogado-geral salientou no nº 141 das suas conclusões, a expressão 'nível de proteção adequado' 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. Com efeito, na falta de uma exigência desta natureza, o objetivo referido no número anterior do presente acórdão seria ignorado. Além disso, o elevado nível de proteção garantido pela Diretiva 95/46, lida à luz da Carta, poderia ser facilmente contornado através de transferências de dados pessoais da União para países terceiros com vista ao seu tratamento nesses países.

À luz desse julgado, MELTZER e MATTOO (2017, p. 776) apontam que “Essa equivalência se refere não apenas ao nível de proteção de dados, mas também se o acesso de agências governamentais a dados pessoais e os direitos de reparação do titular dos dados são consistentes com o GDPR”[112].

Atualmente, há decisões de adequação vigentes para Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, Suíça, Uruguai e Estados Unidos da América (limitado ao *Privacy Shield*, acordo sobre privacidade e proteção de dados pessoais firmado entre EUA e UE).

Na falta de uma decisão de adequação, as transferências internacionais de dados podem ser realizadas com base em outros mecanismos alternativos que prevejam as garantias adequadas em matéria de proteção de dados, os quais necessitam de aprovação da Comissão Europeia ou de uma autoridade de privacidade de um Estado Membro.

O primeiro deles são as chamadas Regras Corporativas Vinculantes (RCV), regras internas de proteção de dados pessoais aplicadas às transferências de dados entre empresas pertencentes ao mesmo grupo econômico. A definição de grupo econômico está contida no item n° 37 do preâmbulo do GDPR:

> Um grupo empresarial deverá abranger uma empresa que exerce o controle e as empresas que controla, devendo a primeira ser a que pode exercer uma influência dominante sobre as outras empresas, por exemplo, em virtude da propriedade, da participação financeira ou das regras que a regem ou da faculdade de fazer aplicar as regras relativas à proteção de dados pessoais. Uma empresa que controla o tratamento dos dados pessoais nas empresas a ela associadas deverá ser considerada, juntamente com essas empresas, um “grupo empresarial”.

Sempre que o tratamento dos dados seja efetuado por um grupo econômico, a sede da empresa controladora deverá ser considerada o estabelecimento principal do grupo, exceto quando as finalidades e os meios do tratamento sejam determinados por uma outra empresa.

---

[112] Tradução livre do original em inglês:” This equivalence relates not only to the level of data protection but also to whether the access of government agencies to personal data and data subject’s rights of redress are consistent with the GDPR”.

As RCVs tomam a forma de um conjunto de documentos internos, que contêm uma obrigação unilateral, possibilitando que empresas multinacionais, organizações internacionais e grupos econômicos realizem transferências internacionais de dados em conformidade com o GDPR.

O objetivo das RCVs é introduzir regras uniformes para o tratamento de dados pessoais aplicáveis às empresas pertencentes ao mesmo grupo econômico, garantindo, assim, um nível adequado de proteção.

Conforme o Artigo 47(1) e (2) do GDPR, as RCVs devem ser juridicamente vinculantes e aplicáveis a todas as empresas do grupo econômico, incluindo os seus funcionários, as quais deverão assegurar o seu cumprimento; conferir direitos aplicáveis aos titulares dos dados; e especificar, necessariamente: **(a)** a estrutura e os contatos das empresas envolvidas; **(b)** a aplicação dos princípios gerais de proteção de dados; **(c)** as transferências ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão; **(d)** o seu caráter juridicamente vinculativo, a nível interno e externo; **(e)** a aplicação dos princípios gerais de proteção de dados; **(f)** os direitos dos titulares dos dados relativamente ao tratamento e regras de exercício desses direitos; **(g)** a aceitação, por parte do responsável pelo tratamento ou subcontratante estabelecido no território de um Estado-Membro, da responsabilidade por toda e qualquer violação das RCVs cometida por uma entidade envolvida que não se encontre estabelecida na União Europeia; **(h)** a forma como as informações sobre as RCVs são comunicadas aos titulares dos dados; **(i)** as funções de qualquer encarregado da proteção de dados e pela supervisão das ações de formação e do tratamento de reclamações; **(j)** os procedimentos de reclamação; **(k)** os procedimentos existentes para assegurar a verificação do cumprimento das RCVs; **(l)** os procedimentos de elaboração de relatórios e de registo de alterações às regras, bem como de comunicação dessas alterações à autoridade de controle; **(m)** o procedimento de cooperação com a autoridade de controle para assegurar o cumprimento; **(n)** ações de formação especificamente dirigidas a pessoas que tenham, em permanência ou regularmente, acesso a dados de natureza pessoal; e **(o)** os procedimentos de comunicação, à autoridade de controle competente, de todos os requisitos legais a que uma empresa

esteja sujeita num país terceiro que sejam passíveis de ter forte impacto negativo nas garantias dadas pelas regras vinculativas aplicáveis às empresas.

Uma alternativa às RCVs é a utilização de códigos de conduta. As associações ou outras entidades que representem categorias de responsáveis pelo tratamento são incentivadas a elaborar códigos de conduta, com o objetivo de facilitar a aplicação do GDPR, tendo em conta as características específicas do tratamento efetuado em determinados setores e as necessidades específicas das micro, pequenas e médias empresas.

Durante o processo de elaboração de um código de conduta, ou na sua alteração ou aditamento, as associações e outros organismos representantes de categorias de responsáveis pelo tratamento deverão consultar as partes interessadas, especialmente os titulares dos dados, se possível, e ter em conta as contribuições recebidas e as opiniões expressas em resposta a essas consultas.

As cláusulas contratuais padrão também permitem a transferência de dados pessoais para países terceiros ou organismos internacionais. Essas cláusulas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, especialmente o direito de recurso administrativo ou judicial e de exigir indenização.

A possibilidade de utilização cláusulas-padrão contratuais é importante para ajudar a agilizar e simplificar o processo de transferência de dados. No entanto, os contratantes poderão acrescentar outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas-padrão adotadas pela Comissão ou por uma autoridade de controle, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados.

Até agora, a Comissão Europeia publicou dois conjuntos de cláusulas-padrão contratuais para transferências de dados entre controladores estabelecidos na União Europeia e controladores estabelecidos fora da União Europeia (Decisão 2001/497/EC e Decisão 2004/915/EC) e um conjunto de cláusulas para transferências de dados de controladores estabelecidos na União Europeia para processadores estabelecidos fora da União Europeia (Decisão 2010/97/EU).

O procedimento de certificação (Artigo 42º, do GDPR) permite o desenvolvimento de selos e marcas de proteção de dados para demonstrar a conformidade com o GDPR por agentes de tratamento dentro da União Europeia.

De acordo com o item b° 100 do preâmbulo do GDPR, a criação de procedimentos de certificação e selos e marcas de proteção de dados tem por objetivo possibilitar aos titulares avaliar rapidamente o nível de proteção de dados dos produtos e serviços que lhes são oferecidos:

> (100) A fim de reforçar a transparência e o cumprimento do presente regulamento, deverá ser encorajada a criação de procedimentos de certificação e selos e marcas de proteção de dados, que permitam aos titulares avaliar rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa.

Por fim, sob reserva de autorização da autoridade de controle competente, podem também ser previstas as garantias adequadas por meio de cláusulas contratuais ou inclusão de dispositivos em acordos administrativos firmados entre as autoridades ou organismos públicos que contemplem os direitos efetivos e oponíveis dos titulares dos dados.

Essas medidas deverão assegurar o cumprimento dos requisitos relativos à proteção de dados e o respeito pelos direitos dos titulares dos dados adequados ao tratamento no território da União Europeia, incluindo a existência de direitos do titular de dados e de medidas jurídicas corretivas eficazes, como o direito de recurso administrativo ou judicial e de exigir indenização, quer no território da União Europeia quer num país terceiro.

2.6.2. APEC Cross-Border Privacy Rules (CBPR) System

A APEC desenvolveu várias iniciativas recentes de proteção de dados, sendo as principais: **(a)** um conjunto de princípios comuns de privacidade; **(b)** um sistema para coordenar reclamações que envolvam mais de uma jurisdição da APEC; e **(c)** o sistema CBPR, uma estrutura de políticas projetada para garantir o fluxo livre e contínuo de informações pessoais através das fronteiras e, ao mesmo tempo, estabelecendo uma proteção significativa para a privacidade e segurança das informações pessoais.

Esta terceira iniciativa é a mais relevante para este estudo, pois tem um impacto direto na interoperabilidade e na transferência internacional de dados pessoais.

O APEC CBPR System é conjunto voluntário de padrões projetados para proteger dados pessoais transferidos para fora dos Estados Membros da APEC pelo uso do princípio de responsabilidade. O sistema CBPR não substitui nem altera as leis e regulamentos nacionais. Por outro lado, onde não há requisitos de proteção de privacidade aplicáveis, o sistema CBPR visa fornecer um nível mínimo de proteção.

O sistema visa facilitar os fluxos internacionais de dados, fornecendo uma estrutura voluntária para garantir segurança e proteção mínima à privacidade. O sistema equilibra o fluxo de informações e dados através das fronteiras e, ao mesmo tempo, fornece proteção eficaz para informações pessoais, essenciais para a confiança no mercado online.

Além disso, o sistema também permite que empresas adotem tais padrões como forma de aplicar proteções em toda a organização, independentemente de onde os dados sejam processados. As empresas que operam na região da APEC são avaliadas e certificadas por um agente de responsabilidade e seguem um conjunto de regras comumente acordadas, com base na Política de Privacidade da APEC.

O sistema CBPR baseia-se na autoavaliação de uma organização de suas políticas e práticas de privacidade de dados em relação aos requisitos da Política de Privacidade da APEC, através de um questionário reconhecido pela própria APEC. Este questionário será fornecido pelo agente de responsabilidade, de acordo com os requisitos de seleção estabelecidos. Conforme o Princípio IX (Responsabilidade):

> Um controlador de informações pessoais deve ser responsável pelo cumprimento das medidas que efetivam os Princípios mencionados acima. Quando as informações pessoais devem ser transferidas para outra pessoa ou organização, nacional ou internacionalmente, o controlador de informações pessoais deve obter o consentimento do indivíduo ou exercer a devida diligência e tomar medidas razoáveis para garantir que a pessoa ou organização receptora proteja as informações de maneira consistente. com esses princípios.

O sistema possui como pontos fortes a associação ampla e diversificada, de modo que há potencial para o esquema atingir um mercado enorme; ser uma das poucas iniciativas de proteção de dados que envolvem têm o apoio dos EUA; e dispor de maior flexibilidade em sua implementação (UNCTAD, 2016, p. 35).

De fato, o sistema concede aos países flexibilidade considerável para implementá-la de uma maneira que leve em consideração suas diferenças sociais, culturais e outras (KUNER, 2013, p. 97). Ao aplicar esse conjunto de regras de base comumente acordado, o sistema CBPR faz a ponte entre diferenças domésticas que podem existir entre as abordagens de privacidade doméstica.

Por outro lado, há claras limitações (UNCTAD, 2016, p. 35), pois o sistema é totalmente voluntário; exige registro de empresas e cobra taxas anuais, o que pode ser considerado um empecilho à adesão ao sistema; e ainda existem regras domésticas de privacidade que acabam se sobrepondo às regras da APEC.

2.6.3. Comunidade Econômica dos Estados da África Ocidental (ECOWAS)

Em fevereiro de 2010, a Comunidade Econômica dos Estados da África Ocidental (ECOWAS, do inglês *Economic Community of West African States*) adotou uma Lei Complementar sobre Proteção de Dados Pessoais, que é uma lei modelo de privacidade que os Estados membros podem adotar (KUNER, 2013, p. 98).

As regras sobre transferência internacional de dados estão previstas no artigo 36:

> 1) O responsável pelo tratamento dos dados deve transferir dados pessoais para um país não membro da CEDEAO apenas onde esse país forneça um nível adequado de proteção à privacidade, às liberdades e aos direitos fundamentais dos indivíduos em relação ao processamento ou possível processamento desses dados.
> 2) O responsável pelo tratamento dos dados deve informar a Autoridade de Proteção de Dados antes de qualquer transferência de dados pessoais para esse país terceiro.

2.7. Brasil

No Brasil, à semelhança do que ocorre com a União Europeia, o direito à privacidade também possui status de direito fundamental. Elencados no art. 5º da Constituição Federal, os direitos fundamentais possuem a natureza de cláusulas pétreas e, por isso, têm em si a garantia de não serem mais revistos, tornando-se definitivos e sem chance de serem diminuídos ou excluídos, salvo mediante a formação de uma nova constituinte e promulgação de uma nova Constituição Federal.

Nos termos do art. 5º, X e XII, da CF/88, são invioláveis “a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” e “o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas (...)”.

Relativamente à proteção de dados, está em tramitação a Proposta de Emenda Constitucional (PEC) nº 17/2019, que inclui a proteção de dados como um dos direitos fundamentais do cidadão bem como fixa a competência privativa da União para legislar sobre a matéria.

Elencar a proteção de dados ao rol taxativo dos direitos fundamentais tem diversos efeitos jurídicos e comerciais. Juridicamente, passa a ter garantia constitucional, e faz com que toda e qualquer discussão sobre regulação do tema seja federal, impedindo, assim, Estados e municípios de criarem regras próprias, sobrepostas e confusas, que causam insegurança jurídica. Analisando a questão sob o viés comercial, o tratamento uniforme e federativo sobre os dados certamente levará em aspectos práticos, evitando assim que empresas presentes em diversos Estados e cidades tenham que se adaptar a um regramento esparso - o que implicaria em um investimento muitas vezes incompatível com o que seria a atividade principal da empresa.

Até recentemente, a proteção da privacidade e dos dados pessoais pela legislação infraconstitucional se dava de forma esparsa e setorizada, a exemplo do Código de Defesa do Consumidor (Lei nº 8.078, de 11 de setembro de 1990), do Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) e da Lei de Acesso à Informação (Lei nº 12.527, de 18 de novembro de 2011, embora em nenhuma deles houvesse disposições relativas às transferências internacionais de dados.

Inspirada na GDPR da União Europeia, a LGPD impôs uma profunda transformação no sistema de proteção de dados brasileiro, em boa medida alinhada com a regulação europeia de proteção de dados.

Trata-se de lei que estabelece regras detalhadas para a coleta, uso, tratamento e armazenamento de dados pessoais e afetará todos os setores da economia, inclusive relações comerciais transnacionais. A LGPD não revoga outras normas protetivas da privacidade e dos dados pessoais; pelo contrário, suas regras e princípios visam, justamente, fortalecer o marco regulatório anteriormente vigente.

Em linhas gerais, a LGPD somente permite a transferência internacional se os mesmos padrões previstos na lei para a proteção ao titular de dados forem mantidos, ou seja, se o país ou organismo internacional oferecer um nível adequado de proteção de dados.

A LGPD determina expressamente as hipóteses em que é permitida a transferência internacional de dados, quais sejam: **(a)** para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado; **(b)** quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na Lei, através de cláusulas contratuais específicas para determinada transferência, cláusulas-padrão contratuais, normas corporativas globais ou selos, certificados e códigos de conduta regularmente emitidos; **(c)** 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; **(d)** quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro; **(e)** quando a autoridade nacional autorizar a transferência; **(f)** quando a transferência resultar em compromisso assumido em acordo de cooperação internacional; **(g)** quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público; **(i)** 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; **(j)** para exercício regular de direitos em processo judicial, administrativo ou arbitral.

Não obstante, o nível de proteção dos dados do país estrangeiro ou do organismo internacional será avaliado pela autoridade nacional de proteção de dados que observará, dentre outras hipóteses, a adoção de medidas de segurança, a natureza dos dados e as normas gerais vigentes no país de destino ou no organismo internacional.

3. PERSPECTIVAS PARA A INTERNACIONALIZAÇÃO DAS NORMAS SOBRE PROTEÇÃO E TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

3.1. Aspectos gerais

Embora seja fora de dúvidas a necessidade potencial de controlar o fluxo internacional de dados para fins de proteção da privacidade, a aplicação de tais controles em um mundo cada vez mais interconectado é muito desafiadora.

Os países fizeram pouco progresso substancial na criação de uma estrutura para resolver os muitos conflitos sobre as políticas da Internet que inevitavelmente ocorrem entre nações soberanas que compartilham acesso a um meio global, apesar do fato de a Internet se tornar mais importante para a sociedade e a economia global a cada dia.

Uma das principais razões para a falta de progresso na política global da Internet é que os países têm valores e prioridades diferentes, e as tentativas de resolver disputas políticas inevitavelmente fracassam porque as várias partes carecem de uma base comum para o diálogo.

De fato, a diversidade de atores, normas e objetivos dificulta a construção de um marco regulatório abrangente que possa acomodar todas as questões jurídicas e interesses envolvidos no que se refere à proteção e transferência internacional de dados pessoais (KUNER, 2013, p. 21).

De um lado, os Estados se mostraram incapazes de formatar um instrumento jurídico abrangente, que pudesse fornecer uma base sólida para regulação a nível internacional; de outro, os instrumentos contratuais (cláusulas contratuais específicas para determinadas transferências; cláusulas-padrão contratuais; normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos), frequentemente utilizados pelo setor privado, não são reconhecidos em todos os sistemas jurídicos, potencializando o risco de conflito (KUNER, 2013, p. 159). Nesse sentido, para CORY, ATKINSON e CASTRO (2019, p 4):

> Isso significa que a Internet, como todas as outras tecnologias, acabou sendo guiada por regras formais e informais por órgãos internacionais, nacionais e subnacionais (governo ou não-governo) ao longo de sua história. O resultado

> é uma colcha de retalhos descoordenada de leis, tratados, regulamentos, normas e padrões. Elas geralmente entram em conflito entre si, especialmente porque as decisões políticas em um país podem criar externalidades negativas significativas para indivíduos e empresas fora desse país - um efeito que provavelmente não será levado em consideração. Ou uma nação pode aprovar uma lei que afeta empresas e indivíduos fora de sua jurisdição e é simplesmente inexequível. De uma perspectiva comercial e econômica, as disputas sobre essas políticas e abordagens podem ser usadas como cobertura para ações essencialmente anticoncorrenciais e que distorcem o comércio que prejudicam a economia global. Quando isso acontece, muitos indivíduos e organizações podem ser pegos no meio[113-114].

Os recentes desenvolvimentos em TIC, como serviços em nuvem, tornam essa tarefa ainda mais complexa. Embora a solução possa eventualmente partir da área de tecnologia (KUNER, 2013, p. 159), a utilização de mecanismos de aproximação jurídica[115], objetivando atingir gradualmente uma melhor interface entre

---

[113] Tradução livre do original em inglês: "This means the Internet, like all other technologies, has ended up being guided by both formal and informal rules by international, national, and subnational bodies (whether government or nongovernment) throughout its history. The result is an uncoordinated patchwork of laws, treaties, regulations, norms, and standards. These often come into conflict with each other, especially as policy decisions in one country can create significant negative externalities for individuals and businesses outside of that country—an effect not likely to be taken into consideration. Or a nation may pass a law that impacts firms and individuals outside of its jurisdiction and is simply unenforceable. From a trade and economic perspective, disputes over these policies and approaches can be used as cover for what are essentially anticompetitive, trade-distorting actions that harm the global economy. When this happens, many individuals and organizations can be caught in the middle".

[114] Sobre a chamada *Lex Informática*, ver COSTA, 2016, p. 162-180). Para a autora, "Aqueles que querem fugir ao ordenamento jurídico dos Estados, criando normas próprias, não poderiam ter encontrado ambiente mais favorável do que a internet, pois, à medida que se multiplicam os usuários e com a velocidade que as informações trafegam na rede, torna-se praticamente impossível rastrear, identificar, tipificar e punir todos os atos em desacordo com a legislação de um Estado. Além disso, tendo em vista as diferenças normativas entre os países e as consequências aterritoriais inerentes ao mundo virtual, o controle de aplicação das normas juspositivistas depende de acordos de cooperação jurisdicional que, quando existem, demandam um longo e custoso processo judicial e diplomático. (...) Tais respostas da legislação nacional, no entanto, ainda não atendem adequadamente a diversas questões e a tendência é que, com a formação cada vez mais frequente das comunidades virtuais de usuários criando produtos e obras em regime de inovação aberta (*open inovation*), cocriação (*crowdcreation* e *crowdsourcing*) e coinvestimento (*crowdfunding*), essas respostas típicas do juspositivismo sejam ainda mais ineficientes".

[115] Os mecanismos de aproximação jurídica são a harmonização, a unificação e a uniformização do direito. De acordo com VICENTE (2008, p. 567 e 568), "Por harmonização de Direitos entendemos a redução das diferenças que os separam quanto a certas matérias, tendo em vista assegurar um certo grau de equivalência funcional entre as soluções neles consagradas, mas sem que seja inteiramente suprimida a diversidade das respectivas regras. (...) Já a unificação de Direitos tem por objetivo a supressão das diferenças entre os sistemas jurídicos considerados, o que pressupõe a identidade das suas regras jurídicas e porventura mesmo a atribuição a um único órgão da competência para decidir em última instância as questões suscitadas pela respectiva interpretação e integração". Além da harmonização e unificação, GAMA JR. (2006, p. 182 e 185) apresenta uma categoria intermediária, a uniformização: "(...) a harmonização jurídica diz respeito ao processo de aproximação das normas de conflito – isto é, das normas clássicas de direito internacional privado – deixando intocadas as normas

os diferentes sistemas regulatórios, tem o potencial de mitigar os efeitos da diversidade jurídica.

Além dos problemas óbvios à privacidade e segurança dos dados pessoais, essa incapacidade de convergência também traz consequências econômicas. Nesse sentido, CHIVOT e CASTRO (2019) identificaram vários problemas causados pela aplicação do GDPR.

A necessidade de se estabelecer uma regulamentação global sobre proteção e transferência internacional de dados pessoais também é identificada por CORY, ATKINSON e CASTRO (2019). Ao fazer um interessante paralelo entre o movimento experimentado no pós-Segunda Guerra Mundial e o surgimento das instituições de Bretton Woods, os autores apontam que:

> Assim como houve um conjunto de instituições, acordos e princípios que surgiram de Bretton Woods após a Segunda Guerra Mundial para gerenciar questões econômicas globais, os países que valorizam o papel de um digital global aberto, competitivo e baseado em regras a economia precisa se unir para aprovar novas regras e normas globais para gerenciar um fator-chave da economia global de hoje: dados[116].

Para eles, o que é necessário é uma estrutura que permita aos países o direito de elaborar políticas da Internet de acordo com suas próprias necessidades e regras nacionais, evitar atropelar os direitos de outras nações soberanas e desenvolver soluções comuns para resolver questões em que existe amplo consenso global (CORY, ATKINSON e CASTRO, 2019, p. 5).

---

nacionais de direito matéria. Esse processo confere maior previsibilidade à solução de conflitos, porquanto o direito aplicável, segundo as regras do direito internacional privado, tende a ser o mesmo, não importando o país em que se trave a disputa. Representa, igualmente, uma iniciativa de concretização mais simples, tanto teórica quanto conceitualmente, já que as normas conflituais circunscrevem-se, em regra, a uns poucos preceitos do direito nacional, com repercussão apenas indireta sobre o conjunto de normas materiais. De outro lado, a unificação jurídica representa a eliminação do contraste normativo entre normas conflituais ou materiais, substituindo-se parcialmente o direito nacional por normas uniformes sobre determinado tema, acertadas entre diferentes países, geralmente por meio de uma convenção ou tratado internacional. (...) Sobre o conceito de uniformização, diz-se que 'tem dupla implicação e variável dimensão', pois representa a combinação possível entre elementos de direito internacional privado e de direito material, tendo maior flexibilidade e alcance que a harmonização, porém menor extensão que a unificação".

[116] Tradução livre do original em inglês: "Just as there was a set of institutions, agreements, and principles that emerged out of Bretton Woods in the aftermath of World War II to manage global economic issues, the countries that value the role of an open, competitive, and rules-based global digital economy need to come together to enact new global rules and norms to manage a key driver of today's global economy: data".

Nesse contexto, três abordagens principais dominam o debate acadêmico atual: a construção de um marco regulatório global em matéria de proteção e transferência internacional de dados pessoais através da harmonização jurídica; a modernização dos acordos da OMC; e a celebração de um tratado internacional específico sobre a matéria.

3.2. Convergência regulatória internacional pela harmonização jurídica

A construção de um marco regulatório global em matéria de proteção e transferência internacional de dados pessoais através da harmonização jurídica é defendida, principalmente, por KUNER (2013, p. 160 e 161) para quem "[A] regulação do fluxo internacional de dados é mais bem compreendida como uma forma de pluralismo jurídico"[117], pois:

> A abordagem pluralista é apropriada quando não há um sistema normativo hierárquico que possa fornecer uma estrutura de governança geral e autorizada, como é o caso da regulação do fluxo internacional de dados.
> (...)
> É, pois, baseada na acomodação entre dois sistemas, e não numa clara hierarquia entre eles.
> (...)
> No sistema pluralista, não existe uma norma hierarquicamente superior (uma norma fundamental [Hans Kelsen] ou regra de reconhecimento [H. L. A. Hart]) que permita a resolução de conflitos, que é precisamente a situação em relação à regulamentação dos fluxos internacionais de dados[118].

Dentre as vantagens da abordagem pluralista, KUNER (2013, p. 164 e 165) destaca a possibilidade de uma harmonização gradual ao longo do tempo, a utilização eficiente de recursos e a prevenção do que ele chama de "encobrimento de disputas", situação em que governantes celebram acordos como forma de legitimar juridicamente determinadas decisões políticas.

---

[117] Tradução livre do original em inglês: "Transborder data flow regulation is best understood as a form of legal pluralism".

[118] Tradução livre do original em inglês: "A pluralist approach is appropriate when there is no hierarchical legal structure that can provide an overall, authoritative governance framework, which is the case with regard to transborder data glow regulation. (…) It is thus based not on a clear hierarchy between the two systems, but on accommodation between them. (…) In a pluralist system, there is no overriding top-level norm (a *Grundnorm* or rule of recognition) that would allow resolution of conflicts, which is precisely the situation with regard to regulation of transborder data flows".

A despeito disso, o KUNER (2013, p. 165) reconhece que a harmonização também possui desvantagens, não podendo ser considerada um fim em si mesmo, bem como que não se deve desconsiderar completamente a opção pelo que ele chama de "solução constitucional", isto é, a celebração de acordos internacionais, não obstante as dificuldades inerentes desta última abordagem:

> O status da regulação do fluxo internacional de dados como um exemplo do pluralismo jurídico não significa que a situação atual é ideal, ou que nada deva ser modificado. Pelo contrário, o *status quo* evidencia inúmeros problemas, incluindo Estados que não levam em consideração a natureza da regulação da proteção de dados; governos que compartilham dados entre si com fundamento em normas legais vagas e imprecisas; regulações excessivamente complexas e promulgadas sem a mínima relação com suas políticas subjacentes; controladores de dados que utilizam politicas de privacidade obscuras; e indivíduos que parecem confusos sobre os fluxos internacionais de dados. A aceitação de um marco legal pluralista não significa que se deva descartar a utilização de mecanismos constitucionais, a exemplo dos acordos internacionais, mas apenas que eles não fornecem uma solução completa[119].

Com isso em mente, KUNER (2013) apresenta oito sugestões que ele considera necessárias para o melhoramento do marco regulatório da proteção e transferência internacional de dados atualmente existe.

Em primeiro lugar, o autor entende que a regulação não deve exigir bases legais específicas para permitir as transferências internacionais de dados, nem submetê-las a aprovação prévia das autoridades reguladoras, devendo lhes ser aplicadas as mesmas bases legais exigidas para o tratamento dos dados pessoais, com a previsão de poderes específicos para as autoridades reguladoras suspenderem tais transferências ou sujeita-las a condições especiais em determinadas circunstâncias.

Dentro da tipologia regulatória proposta por CASALINI e GONZÁLEZ (2019)[120], essa abordagem, chamada pelo autor de "regra padrão" ("*default rule*")

---

[119] Tradução livre do original em inglês: "The status of transborder data flow regulation as an example of legal pluralism does not mean that the current situation is ideal, or that nothing should be changed. On the contrary, the *status quo* evidences a number of problems, including States that do not adequately take into account the transborder nature of data protection regulation; governments that share data between themselves under murky legal rules; regulation that is overly complex and enacted without sufficient regard to its underlying privacy policies; data controllers that use unclear privacy policies; and individuals who seem ambivalent about transborder data flows. Acceptance of a pluralist legal framework does not mean that constitutional mechanisms such as international agreements should never be pursued, but does demonstrate that they cannot provide a complete solution".

[120] A classificação desenvolvida por CASALINI e GONZÁLEZ (2019) foi detalhada no capítulo 2.

poderia ser enquadrada na terceira categoria, a dos chamados “fluxos condicionados a salvaguardas”. Embora o autor não deixe claro o nível desejado de intervenção das autoridades regulatórias nesse processo, como ele defende uma atuação estatal mínima, pode-se considerar que essa abordagem se aproxima mais da primeira subcategoria os “fluxos condicionados a salvaguardas”, em que as bases legais para a transferência internacional de dados são previamente estabelecidas, mas cabe aos próprios agentes de tratamento, e não ao Estado, verificar ou não o seu cumprimento.

Embora confira maior flexibilidade às empresas, na medida em que delega aos particulares poderes de avaliação e decisão sobre a realização ou não da transferência internacional de dados, essa abordagem também aumenta os riscos das empresas, uma vez que elas se tornam responsáveis pelas transferências e eventuais violações aos direitos dos titulares.

A LGPD não se alinha à ideia defendida por KUNER (2013). Dos onze casos em que é permitida a transferência internacional de dados (art. 33 da LGPD), apenas cinco[121] coincidem com as hipóteses de tratamento de dados pessoais taxativamente previstas no art. 7º da LGPD.

A aplicação das mesmas bases legais do tratamento às transferências internacionais de dados permitiria sua ocorrência sem a necessidade de anuência prévia da autoridade reguladora, de modo que o controle do cumprimento das determinações legais ocorreria *a posteriori*.

Ao transferir para as empresas a responsabilidade pela legitimidade das transferências internacionais de dados, essa medida vai ao encontro da segunda e terceira medidas sugeridas por KUNER (2013, p. 157 e 173), a “abordagem organizacional com a geografia como fator relevante” e a “responsabilidade contínua dos controladores de dados”, isto é, da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

[121] São eles: mediante o fornecimento de consentimento pelo titular dos dados; para o cumprimento de obrigação legal ou regulatória pelo controlador; quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do quão seja parte o titular, a pedido do titular dos dados; para o exercício regular de direitos em processo judicial, administrativo ou arbitral; e para a proteção da vida ou da incolumidade física do titular ou de terceiro.

A segunda medida se refere à combinação entre as abordagens organizacional e geográfica, uma terceira via alternativa à classificação tradicional[122]. Nesta abordagem, embora ainda seja relevante, "(...) uma vez que os seres humanos tendem a se agrupar geograficamente, com base em culturas, idiomas, gostos, riqueza e valores comuns"[123] (KUNER, 2013, p. 170), a questão geográfica agora é apenas um dos vários elementos levados em consideração no momento da tomada da decisão empresarial sobre a legitimidade de uma transferência internacional de dados específica. Nas palavras de KUNER (2013, p. 172):

> Nesta abordagem, o local de destino dos dados não é o único fator determinante para se considerar uma transferência apropriada, mas um dos elementos a serem levados em consideração numa análise de risco baseada no nível de sensibilidade das informações pessoais, a expectativa dos titulares dos dados, e o potencial dano se os as informações pessoais forem indevidamente vazadas ou utilizadas de maneira equivocada[124].

Nesse mesmo sentido, CORY, ATKINSON e CASTRO (2019, p. 8) defendem que os formuladores de políticas precisam se concentrar em uma abordagem baseada em responsabilidade, em vez de acreditar erroneamente que forçar as empresas a armazenar dados em determinado local é a forma de proteger dados pessoais.

Quando se trata de manipulação de dados, as empresas que fazem negócios em um país devem ser responsáveis e responsabilizadas de acordo com as leis e os regulamentos do país, por suas próprias ações e pelas ações de seus agentes e parceiros de negócios, independentemente de estarem localizadas fora do país onde uma empresa coleta ou gerencia dados. Portanto, o foco dos formuladores de políticas na elaboração de leis e regulamentos relativos à proteção e transferência internacional de dados deve ser garantir a responsabilização das empresas, independentemente de onde elas armazenem, processem ou para onde transfiram os dados.

Assim, pela terceira medida, os controladores devem permanecer responsáveis pelo tratamento irregular dos dados, seja pela inobservância da

---

[122] A distinção foi detalhada no capítulo 2.

[123] Tradução livre do original em inglês: "(...) since human beings tend to cluster geographically, based on shared cultures, languages, tastes, wealth, and values".

[124] Tradução livre do original em inglês: "Under this approach, the location to which data are exported is not the sole consideration in determining whether a transfer is appropriate, but is one factor to be considered in a risk analysis based on the sensitivity of the personal information, the expectations of the individuals to whom the information relates, and the potential injury if personal information is wrongly disclosed or misused".

legislação, seja pelo não fornecimento da segurança necessária, assim considerada a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, mesmo após a sua transferência para outros países, inclusive com a previsão de penalidades.

Esse princípio da responsabilidade baseia-se em dois pontos principais: uma empresa com vínculo jurídico na jurisdição de um país deve cumprir suas leis relacionadas a dados (mesmo que a empresa transfira dados para o exterior), e a governança de dados doméstica de cada país precisa ser global no escopo e na interoperabilidade, dada a natureza globalmente distribuída da internet.

Primeiro, os formuladores de políticas devem se concentrar em garantir que suas estruturas legais deixem claro que as empresas com um nexo legal em sua jurisdição são responsáveis por gerenciar dados de uma certa maneira, onde quer que os dados sejam transferidos e armazenados.

As empresas que fazem negócios em um determinado país teriam um forte incentivo para ajudar seus parceiros de negócios fora desse país a aderirem às suas proteções de privacidade, porque seus cidadãos e o governo poderiam buscar soluções dessa empresa para qualquer violação de privacidade, como violação de dados, independentemente de a empresa ou seus parceiros estarem em falta.

Segundo esse princípio de responsabilidade baseia-se no fato de que a tecnologia moderna, especialmente a internet e o armazenamento de dados, significa que os regimes regulatórios nacionais precisam ser globalmente interoperáveis, dado que cada país enfrenta o mesmo desafio na aplicação de suas leis a empresas que possam transferir dados entre jurisdições. As estruturas de privacidade interoperáveis são a extensão internacional dessa abordagem baseada em responsabilidade, de modo que os dados ainda possam fluir entre diferentes regimes de privacidade e as regras de proteção de dados dos países fluem com eles.

Os formuladores de políticas devem aplicar uma abordagem baseada em responsabilidade para garantir que as empresas forneçam acesso oportuno aos dados em resposta a solicitações de dados das autoridades reguladoras financeiras, em vez de se concentrarem no local de armazenamento de dados. Para CORY, ATKINSON e CASTRO (2019, p. 3):

> Em vez de dizer às empresas onde elas podem armazenar ou processar dados, os formuladores de políticas devem responsabilizar as empresas pelo gerenciamento dos dados que coletam, independentemente de onde eles os armazenam ou processam. As principais economias digitais precisam articular e aprovar uma estrutura baseada na responsabilidade e interoperabilidade local, a fim de fornecer uma alternativa mais clara e melhor às duas outras abordagens principais e contrastantes: esforços dos países (principalmente europeus) para fazer com que outros países adotem sua abordagem (universalista) à privacidade dos dados, a fim de torná-los responsáveis pela aplicação (em vez de responsabilizar as empresas), e os países forçando as empresas a armazenar apenas dados localmente (um conceito conhecido como localização de dados)[125].

Em quarto lugar, KUNER (2013, p. 174) defende a adequação das regulações à realidade tecnológica. Como visto, a rapidez com a tecnologia evolui é umas das principais dificuldades na aplicação das normas sobre proteção e transferência internacional de dados. Nesse sentido:

> Se a definição de "transferência de dados" depende do estado da tecnologia em determinado momento, ela se tornará obsoleta rapidamente. Ao invés de definir transferência de dados com base em fatores como se os dados foram "disponibilizados" passivamente ou "transmitidos" voluntariamente, as normas sobre transferência internacional de dados devem ser aplicadas se os dados pessoais forem objeto de tratamento fora do país onde foram originalmente coletados[126].

A quinta sugestão de KUNER (2013, p. 175) é a "promoção da interoperabilidade legal internacional", através da cooperação jurídica intergovernamental e da padronização de mecanismos regulatórios entre os diferentes sistemas jurídicos, a exemplo do artigo 13 da Convenção 108, que possui as seguintes regras sobre cooperação jurídica internacional:

---

[125] Tradução livre do original em inglês: "Rather than tell firms where they can store or process data, policymakers should hold firms accountable for managing data they collect, regardless of where they store or process it. Leading digital economies need to articulate and enact a framework that is based on local accountability and interoperability in order to provide a clearer, and better, alternative to the two other main, contrasting approaches: efforts by (mainly European) countries to make other countries adopt their (universalist) approach to data privacy in order to make them responsible for enforcement (instead of holding firms responsible), and countries forcing firms to only store data locally (a concept known as data localization)".

[126] Tradução livre do original em inglês: "If the definition of a 'data transfer' is made dependent on the state of technology at a particular point in time, it will quickly become outdated. Rather than defining a data transfer based on factors such as whether data were passively 'made available' or actively 'transmitted', the applicability of transborder data flow regulation should be triggered by whether personal data will be processed outside the country where they were originally collected".

> **Artigo 13 – Cooperação entre Partes**
> 1 As Partes acordam em prestar assistência mútua para implementar a presente Convenção.
> 2 Para esse fim:
> a) Cada Parte designará uma ou mais autoridades, cujo nome e endereço serão comunicados ao Secretário-Geral do Conselho da Europa;
> b) cada Parte que designou mais de uma autoridade deve especificar em sua comunicação referida no parágrafo anterior a competência de cada autoridade.
> 3) Uma autoridade designada por uma Parte deverá, a pedido de uma autoridade designada por outra Parte:
> a) fornecer informações sobre sua lei e prática administrativa no campo da proteção de dados;
> b) adote, em conformidade com a legislação nacional e com o único objetivo de proteção da privacidade, todas as medidas apropriadas para fornecer informações factuais relacionadas ao processamento automático específico realizado em seu território, com exceção, porém, dos dados pessoais sendo processados.

Especificamente, KUNER (2013, p. 176-178) defende o reconhecimento de instrumento contratuais (cláusulas contratuais específicas para determinadas transferências; cláusulas-padrão contratuais; normas corporativas globais; selos, certificados e códigos de conduta regularmente emitidos) e mecanismos de responsabilização comuns entre diferentes regiões; concordância sobre hipóteses especificas de transferências internacionais de dados que demandem proteção adicional e medidas técnicas que possam criar incentivos para proteger os dados transferidos internacionalmente; maior cooperação entre autoridades regulatórias de diferentes países [127] ; e a elaboração de uma lei modelo internacional sobre transferência internacional de dados, nos moldes da Lei Modelo sobre Arbitragem Comercial Internacional da Comissão das Nações Unidas para o Direito Internacional do Comércio (UNCITRAL, do inglês *United Nations Commission on International Trade Law*) e dos princípios do Instituto Internacional para a Unificação do Direito Privado, também conhecido como UNIDROIT.

CORY, ATKINSON e CASTRO (2019, p. 3) também defendem que os países devem revisar os procedimentos relativos às solicitações de acesso a dados armazenados em outras jurisdições. Para eles:

> Se quisermos estabelecer um fluxo livre amplamente compartilhado de dados com regime de confiança, um componente essencial dessa confiança deve ser as agências nacionais de aplicação da lei que podem ter acesso a dados

[127] No Brasil, compete à ANPD “promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional” (art. 55-J, IX, da LGPD).

> domésticos (relacionados a investigações legítimas da lei) armazenados em outros países[128].

A sexta sugestão se refere a "limitações jurisdicionais e maior aceitação de valores internacionais". De acordo com KUNER (2013, p. 180 e 181), autoridades regulatórias devem ser mais cautelosas ao reivindicar sua jurisdição em matéria de proteção e transferência internacional de dados pessoais, reconhecendo-se, ao contrário, a existência de valores comuns à comunidade internacional:

> Governos e reguladores devem ser cautelosos ao invocar sua jurisdição e reclamar a aplicação de suas regulações nacionais sobre transferência de dados, e reconhecerem, em circunstâncias especiais, a importância de valores importantes que interessam à toda comunidade internacional como fundamento para a transferência de dados pessoais[129].

Por fim, KUNER (2013, p. 183 e 184) sugere o aumento da transparência entre Estado e controladores de dados e que governos e autoridades regulatórias também observem as normas sobre transferência de dados.

Além das medidas sugeridas por KUNER (2013), outras duas são mencionadas por CORY, ATKINSON e CASTRO (2019).

Primeiramente, partindo da premissa de que nem todos os fluxos de dados devem ser tratados da mesma forma, pois alguns fluxos são ilegais, os autores defendem que os países devem desenvolver estruturas legais e administrativas que permitam aos provedores de serviços da internet bloquearem fluxos de dados que envolvam a distribuição ilegal e o uso de conteúdo não licenciado.

Para eles, "(...) não há nada contraditório em apoiar fortemente o fluxo livre de dados global, além de apoiar o bloqueio do fluxo de dados ilegais, assim como não

---

[128] Tradução livre do original em inglês: "If we are to establish a widely shared free flow of data with trust regime, one key component of that trust needs to be national law enforcement agencies trusting they can get access to domestic data (related to legitimate law enforcement investigations) stored in other nations".

[129] Tradução livre do original em inglês: "Governments and regulators should be cautious in asserting jurisdiction and application of their national transborder data flow regulation, and in appropriate circumstances should recognize important values that are of concern to the entire international community as grounds for transferring personal data".

é apoiar fortemente o livre comércio de mercadorias, ao mesmo tempo em que apoia o bloqueio do comércio de espécies ameaçadas de extinção. ou tráfico de pessoas"[130].

Ademais, os países devem apoiar e não prejudicar o papel da criptografia na proteção de fluxos de dados e tecnologias digitais, para assegurar a "(...) segurança geral de cidadãos e empresas cumpridores da lei, dificulta a concorrência de empresas de países com criptografia enfraquecida nos mercados globais e limita os avanços na segurança da informação" (CORY, ATKINSON e CORY, 2019, p. 4)[131].

3.3. Regulação global via revisão dos acordos da OMC

À medida que o comércio se torna cada mais dependente da internet e das novas tecnologias, normas, regras e procedimentos comerciais precisam ser adaptados ao mundo digital (CIURIAK e PTASHKINA, 2018, p. 2). As regras da OMC também precisam incorporar mecanismos para melhorar a confiança dos negócios e apoiar uma economia baseada em dados.

Nesse sentido, MITCHELL e MISHRA (2019) são os principais defensores da regulação global via revisão dos acordos da OMC. Para eles, a OMC seria o foro adequado para essa discussão porque é o principal organismo internacional que lida com as regras do comércio entre as nações, congregando 164 membros efetivos e 23 com *status* de observadores, além de o comércio eletrônico, que depende diretamente dos fluxos internacionais de dados, ser um dos principais temas de discussão no âmbito da OMC nos últimos (MITCHELL e MISHRA, 2019, p. 3).

Assim, como KUNER (2013), os autores também apresentam uma proposta de marco regulatório para a proteção e transferência internacional de dados, cujo elemento central é a combinação de regras vinculantes sobre transferências internacionais de dados com disposições relativas à proteção do consumidor, privacidade e cibersegurança. Para eles:

---

[130] Tradução livre do original em inglês: "Thus, there is nothing contradictory about strongly supporting the global free flow of data while also supporting the blockage of the flow of illegal data, any more than it is to strongly support the free trade of goods, while supporting the blocking of trade in endangered species or human trafficking".

[131] Tradução livre do original em inglês: "Any government attempt to undermine encryption reduces the overall security of law-abiding citizens and businesses, makes it more difficult for companies from countries with weakened encryption to compete in global markets, and limits advancements in information security".

> Um marco regulatório ideal para o comércio internacional deveria facilitar o livre fluxo de dados, a inovação digital, e a competição sadia no mercado digital global sem interferir no direito dos países de regularem a internet por razões legítimas (MITCHELL e MISHRA, 2019, p. 14)[132] .

Para tal, sugerem a adoção de seis medidas, fundadas no que eles chamam de princípios fundamentais da regulação de dados no comércio internacional.

O primeiro desses princípios é o da promoção da confiança digital em nível doméstico e transnacional (MITCHELL e MISHRA, 2019, p. 15). Embora reconheçam que a OMC pode desempenhar um papel importante na proteção da privacidade dos consumidores, no combate a fraudes e ataques cibernéticos e, por conseguinte, na promoção de novos negócios, entendem que o há limitações na sua atuação, especialmente em razão de o GATS permitir que os Estados Membros adotem medidas domésticas para alcançar os objetivos políticos listados no art. XIV, mesmo que sejam restritivas ao comércio internacional.

Por isso, defendem o aprofundamento do diálogo transnacional e a coordenação e cooperação internacional em questões que incluem fluxos de dados, segurança cibernética e privacidade, entre OMC e outras instituições participantes do eles denominam ecossistema global dos fluxos internacionais de dados, como a *Internet Engineering Task Force* (IETF), *World Wide Web Consortium* (W3C), *Institute of Electrical and Eletronics Engineers* (IEEE), *Internet Corporation for Assigned Names and Numbers* (ICANN) e *International Telecommunications Union* (ITU).

O segundo princípio é o da garantia da interoperabilidade e da transparência para facilitação do livre fluxo de dados (MITCHELL e MISHRA, 2019, p. 15 e 16), que objetiva facilitar os fluxos de dados e a responsabilização no meio digital. Assim como KUNER (2013), para quem a interoperabilidade e a transparência são essenciais à harmonização das normas sobre proteção e transferência internacional de dados, os autores entendem que:

> Aqui, a OMC pode aprender com a experiência de outras instituições como a Comissão das Nações Unidas para o Direito Internacional do Comércio (UNCITRAL) e o Instituto Internacional para a Unificação do Direito Privado (UNIDROIT) que alcançaram a interseção entre diferentes estruturas regulatórias no direito internacional público e privado. Além disso, o

[132] Tradução livre do original em inglês: “An ideal digital trade framework should facilitate free data flows, digital innovation, and healthy competition in the global digital market without interfering with as country’s right to regulate the internet for legitimate reasons”.

> reconhecimento mútuo pode ser incentivado pelo desenvolvimento de novas disciplinas nos termos do art. VI:5 do GATS sobre 'requerimentos e procedimentos de qualificação, padrões técnicos e obtenção de licenças' relativas aos fluxos de dados.
> Outra questão fundamental que deveria ser endereçada nos acordos da OMC é a transparência das regulações de dados. A despeito dos mecanismos legais vinculantes previstos no art. III do GATS, vários Membros adotam medidas restritivas ambíguas, causando considerável incerteza para empresas e consumidores[133].

Em terceiro lugar, MITCHELL e MISHRA (2019, p. 16 e 17) defendem a adoção de novas abordagens regulatórias tanto no que se refere ao comércio digital quanto em matéria de proteção e transferência internacional de dados, as quais devem levar em consideração a natureza multissetorial do regime de governança da internet, principalmente devido ao papel central do setor privado em garantir a abertura e segurança.

Assim como o papel desempenhado pelo FMI em assuntos relativos à moeda e câmbio, e com outras instituições em questões ambientais, os autores consideram que:

> Não há razão para que uma abordagem semelhante não possa ser seguida na área de regulação da Internet e de dados, em que instituições multissetoriais desempenham um papel fundamental. Essa abordagem exigiria cooperação entre a OMC e outras organizações relevantes, como a UIT, e órgãos da Internet, incluindo IETF e ICANN. Além disso, as discussões com várias partes interessadas, envolvendo especialistas em Internet, podem permitir uma avaliação mais equilibrada dos riscos cibernéticos nos serviços digitais e a necessidade de certas medidas restritivas ao comércio para lidar com esses riscos cibernéticos. Essa abordagem será mais eficaz do que as restrições unilaterais de dados que geralmente têm um impacto limitado na garantia de confiança e inovação digitais[134].

---

[133] Tradução livre do original em inglês: "Here, the WTO can learn from the experience of other institutions such as United Nations Commission on International Trade Law ('UNCITRAL') and International Institute for the Unification of Private Law ('UNIDROIT') that have achieved intersections between varying regulatory framework in public and private international law. Further, mutual recognition can be incentivized by developing new disciplines under GATS art. VI:5 on 'qualification requirements and procedures, technical standards and licensing requirements' pertaining to data flows. Another fundamental requirement that should be addressed in WTO law is transparency of data regulations. Despite a binding legal mechanism under GATS art. III, several Members adopt ambiguously worded data restrictive measures, causing considerable uncertainty for businesses and consumers alike".

[134] Tradução livre do original em inglês: "There is no reason why a similar approach cannot be followed in the area of internet and data regulation where multistakeholder institutions play a key role. This approach would require cooperation between the WTO and other relevant organizations such as the ITU as well as multistakeholder internet bodies including IETF and ICANN. Further, multistakeholder discussions involving internet experts can enable a more balanced evaluation of cyber risks in digital services and the necessity of certain trade-restrictive measures to address these cyber risks. This approach will be more effective than unilateral data restrictions that usually have a limited impact on ensuring digital trust and innovation".

Com base nesses princípios fundamentais da regulação de dados no comércio internacional, MITCHELL e MISHRA (2019, p. 17 e 18) sugerem a reforma dos acordos da OMC, de modo a torna-los mais adequados à *data driven economy*, seja através da reforma do GATS, mediante adoção de novos compromissos sobre os fluxos de dados, ou pela negociação de um acordo plurilateral sobre comércio eletrônico compreendendo diferentes questões de comércio digital, incluindo fluxos de dados e requisitos de localização.

Como os fluxos de dados são fundamentais para o crescimento da economia digital e facilitam os negócios em toda a cadeia de suprimentos global, com o objetivo de realizar transações comerciais e proibir medidas de localização de dados, os autores recomendam que os acordos da OMC incorporem uma obrigação horizontal que possibilite as transferências internacionais de dados. Para facilitar a construção de um ambiente aberto e seguro para as transferências internacionais de dados, também consideram necessária a inclusão de disposições sobre segurança cibernética e comércio internacional.

Além disso, os Estados Membros devem adotar um nível básico de regulamentação de segurança cibernética que os impeça de se tornarem refúgios para crimes cibernéticos. Assim, ao invés de formularem ou recomendarem padrões ou melhores práticas domésticas específicas de segurança cibernética, os Estados Membros devem ser incentivados a dar preferência a padrões internacionalmente reconhecidos. Dessa forma, é fundamental a cooperação internacional entre os Estados Membros e organizações não estatais que desempenham um papel fundamental na governança internacional.

A privacidade é necessária para incutir maior confiança digital. A atual estrutura do GATS permite uma exceção para medidas de privacidade, mas essa exceção é insuficiente, pois é improvável que os países de origem dos dados aceitem limites unilaterais ao seu direito de aplicar medidas de segurança cibernética para proteger sua soberania na internet. Em outras palavras, para permitir transferências internacionais de dados, os países de origem e destino devem ter estruturas de privacidade eficazes, de modo que os acordos da OMC devem exigir que todos os Estados Membros adotem uma estrutura regulatória básica para proteção da privacidade, sendo fundamental para garantir o livre fluxo de dados.

A confiança do consumidor é um requisito fundamental para o comércio digital e requer não apenas leis nacionais fortes, mas também cooperação e envolvimento internacional persistente entre as partes interessadas relevantes, como empresas privadas, organizações de defesa do consumidor e agências de proteção ao consumidor.

Nesse sentido, MITCHELL e MISHRA (2019, p. 24) sugerem a adoção pelos Estados Membros de uma estrutura regulatória básica sobre proteção ao consumidor online, incluindo proteção contra práticas comerciais fraudulentas e enganosas, através da incorporação da Lei Modelo da UNCITRAL sobre Comércio Eletrônico pelos acordos da OMC. Ademais, consideram que os Estados Membros devem adotar um mecanismo de cooperação obrigatório para abordar os aspectos transnacionais da proteção ao consumidor online, incluindo o compartilhamento de informações e a prestação de assistência para a aplicação das leis de proteção ao consumidor.

3.4. Disciplinamento da matéria através da celebração de tratado internacional

Embora admitam a possibilidade de melhorar instituições, processos e ferramentas existentes através de tratados de assistência jurídica mútua, CORY, ATKINSON e CASTRO (2019) tratam essas medidas como paliativas, e defendem que os países devem desenvolver uma Convenção de Genebra para Dados que estabeleça regras internacionais de transparência, resolva questões de jurisdição e melhore a cooperação jurídica internacional, sob a seguinte justificativa:

> Idealmente, os países se uniriam para negociar um novo acordo multilateral com a Convenção de Genebra sobre o Status dos Dados para estabelecer regras internacionais de transparência, resolver questões de jurisdição, engendrar cooperação para uma melhor coordenação das solicitações internacionais de aplicação da lei e limitar o acesso desnecessário do governo aos dados. em cidadãos de outros países. Isso também ajudaria os países a seguir regras e procedimentos semelhantes para solicitações de aplicação da lei além das fronteiras, além de limitar o acesso desnecessário do governo a dados de cidadãos de outros países. Isso solicita e ações. com as partes concordando em não aprovar a localização dos dados (pois isso prejudicaria o ponto central do contrato).
> Essa iniciativa multilateral seria baseada na soberania nacional, uma vez que diferentes nações têm diferentes conjuntos de valores, prioridades e sistemas legais. E como as empresas de Internet oferecem serviços através de redes globais, geralmente ocorre que dois ou mais países têm interesse nos mesmos dados. Essa iniciativa não deve forçar as políticas de uma nação em particular, como promover o padrão estrito de causa provável para reunir evidências (como no caso dos Estados Unidos) ou permitir que

> o governo acesse evidências em detrimento das liberdades pessoais (como no caso de nações como China e Rússia), no resto do mundo. Portanto, cada empresa deve estar sujeita às leis de cada país em que possui presença legal. Esse princípio garantiria que nenhuma empresa escapasse ao cumprimento das leis de uma nação simplesmente transferindo dados para o exterior. É simplesmente uma questão de criar uma estrutura para criar interoperabilidade entre as abordagens de diferentes países[135].

De forma diametralmente oposta, KUNER (2013) descarta completamente a possibilidade de utilização de tratado internacional para regulamentar questões relativas à proteção e transferência internacional de dados de pessoais.

Para ele, embora uma convenção multilateral seja vinculativa nos termos do direito internacional, ainda assim pode não produzir um quadro jurídico harmonizado, uma vez que, na maioria dos países, um tratado deve ser implementado na legislação nacional e pode precisar ser comparada com os padrões da lei constitucional, o que pode resultar em diferenças significativas entre as abordagens nacionais. Além disso, um tratado também não necessariamente teria precedência sobre a multiplicidade de leis, regulamentos, instrumentos do setor privado e códigos de práticas nacionais que existem atualmente.

---

[135] Tradução livre do original em inglês: “Ideally, countries would come together to negotiate a new multilateral agreement a Geneva Convention on the Status of Data to establish international rules for transparency, settle questions of jurisdiction, engender cooperation for better coordination of international law enforcement requests, and limit unnecessary government access to data on citizens of other countries. This would also help countries follow similar rules and procedures for cross-border law enforcement requests, and limit unnecessary government access to data on citizens of other countries. This requests and actions. with parties agreeing not to enact data localization (as this would undermine the central point of the agreement).
Such a multilateral initiative would be based on national sovereignty, as different nations have different sets of values, priorities, and legal systems. And because Internet companies offer services over global networks, it is often the case that two or more countries have interests in the same data. This initiative should not force a particular nation’s policies, such as promoting the strict standard of probable cause to gather evidence (as in the case of the United States) or allowing government access to evidence at the detriment of personal freedoms (as in the case of nations such as China and Russia), on the rest of the world. Therefore, each business should be subject to the laws of each country in which they have a legal presence. This principle would ensure no company can escape complying with a nation’s laws by simply transferring data overseas. It is simply a matter of coming up with a framework to create interoperability between different countries’ approaches.”

4. CONSIDERAÇÕES FINAIS

A internet é essencial para o comércio internacional no século XXI. À medida que os comerciantes usam cada vez mais a internet para acessar mercados no exterior, a internet tem o potencial de mudar a maneira como o comércio internacional é conduzido. Por exemplo, a capacidade de adquirir bens e serviços digitais instantaneamente e o desenvolvimento de novas tecnologias, como impressoras 3D, permitem que as empresas eliminem custos de transação, aumentando a competitividade no mercado internacional.

Daí porque o fluxo internacional de dados é um elemento central do que faz da internet a força poderosa para a transmissão de informação e conhecimento e para o desenvolvimento econômico, especialmente porque empresas podem utilizar a internet para exportar bens; serviços podem ser contratados e consumidos *online*; a coleta e a análise de dados permitem que novos serviços agreguem valor às exportações de mercadorias; os fluxos globais de dados sustentam as cadeias de valor globais, criando novas oportunidades de negócios; aumenta-se a concorrência internacional e criam-se novos mercados consumidores.

A despeito disso, é crescente o protecionismo de dados, caracterizado, especialmente, pela imposição de requisitos de localização de servidores em determinadas localidades e pela vedação ou limitação das transferências internacionais de dados

O desafio é estabelecer um nível adequado de proteção da privacidade e dos dados pessoais, sem interferir negativamente no desenvolvimento de novas tecnologias e no crescimento econômico mundial

É necessário, portanto, o desenvolvimento de políticas e regulamentos que possam sustentar e apoiar o impacto transformador da internet e dos fluxos internacionais de dados no comércio internacional, ao mesmo tempo em que se promova uma maior proteção da privacidade e dos dados pessoais.

REFERÊNCIAS

AARONSON, Susan Ariel. Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security. In: **World Trade Review**, v. 14, n. 4, p. 671-700, 2015.

AARONSON, Susan Ariel; LEBLOND, Patrick. Another Digital Divide: The Rise of Data Realms and its Implications for the WTO. In: **Journal of International Economic Law, v. 21**, n. 2, p. 245-272, jun. 2018.

AHMED, Usman; CHANDER, Anupam. **Information goes global: protecting privacy, security and the new economy in a world of cross-border data flows**. E15Initiative. Genebra: International Centre for Trade and Sustainable Development (ICTSD) e World Economic Forum, 2015. Disponível em: www.e15initiative.org. Acesso em 26 jun. 2019.

AHMED, Usman; ALDONAS, Usman. **Addressing barriers to digital trade**. E15Initiative. Genebra: International Centre for Trade and Sustainable Development (ICTSD) e World Economic Forum, 2015. Disponível em: www.e15initiative.org. Acesso em 26 jun. 2019.

ALLEN, Anita L. Protecting one's own privacy in a big data economy. In: **Harvard Law Review**, v. 130, p. 71-78, 2016.

ALTMAN, Micah et al. Practical approaches to big data privacy over time. In: **International Data Privacy Law**, v. 8, n. 1, p. 29-51, fev. 2018.

BALDWIN, Richard. Trade and Industrialization after Globalization's Second Unbundling: How Building and Joining a Supply Chain Are Different and Why It Matters. In: FEENSTRA, Robert; TAYLOR, Alan (eds). **Globalization in an Age of Crisis: Multilateral Economic Cooperation in the Twenty-First Century**. Chicago: University of Chicago Press, 2014.

BARTELS, Lorand. The Chapeau of the General Exceptions in the WTO GATT and GATS Agreements: A Reconstruction. In: **American Journal of International Law**, v. 109, n. 1, p. 95-125, jan. 2015.

BASEDOW, Robert. The WTO and the Rise of Plurilateralism - What Lessons can we Learn from the European Union's Experience with Differentiated Integration? In: **Journal of International Economic Law**, v. 21, n. 2, p. 411-431, jun. 2018.

BATTCOCK, Rupert. Data Protection: where next? In: **International Journal of Law and Information Technology**, v. 3, n. 2, p. 156-178, 1995.

BENVENISTI, Eyal. Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance? In: **European Journal of International Law**, v. 29, n. 1, p. 9-82, fev. 2018.

BIGNAMI, Francesca. Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy. In: **The American Journal of Comparative Law**, v. 59, n. 2, p. 411-461, 2011.

BLUME, P. Transborder data flow: is there a solution in sight? In: **International Journal of Law and Information Technology**, v. 8, n. 1, p. 65-86, 2000.

BOLLYKY, Thomas; MAVROIDIS, Petros. Trade, Social Preferences and Regulatory Cooperation: The New WTO-Think. In: **Journal of International Economic Law**, v. 20, n. 1, p. 1-30, mar. 2017.

BORGHI, Maurizio; FERRETTI, Federico; KARAPAPA, Stavroula. Online data processing consent under EU law: a theoretical framework and empirical evidence from the UK. In: **International Journal of Law and Information Technology**, v. 21, n. 2, p. 109-153, 2013.

BOYNE, Shawn Marie. Data Protection in the United States. In: **The American Journal of Comparative Law**, v. 66, n. 1, p. 299-343, jul. 2018.

BRKAN, M. The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU's Constitutional Reasoning. In: **German Law Journal**, v. 20, n. 6, p. 864-883, 2019.

BROOKINGS INSTITUTE. **The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment** (2014). Disponível em: http://www.brookings.edu/~/media/research/files/papers/2014/10/internet-transatlantic-data- flows-meltzer/internet-transatlantic-data-flows-version-2.pdf. Acesso em: 30 dez. 2019.

BROWN, Ian. The feasibility of transatlantic privacy-protective standards for surveillance. In: **International Journal of Law and Information Technology**, v. 23, n. 1, p. 23-40, 2015.

BURRI, Mira; SCHÄR, Rahel. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. In: **Journal of Information Policy**, v. 6, p. 479-511, jun. 2016.

BURRI, Mira. The regulation of data flows through trade agreements. In: **Georgetown Journal of International Law**, v. 48, n. 1, ago 2017a.

BURRI, Mira. The governance of data and data flows in trade agreements: the pitfalls of legal adaptation. In: **UC Davis Law Review**, v. 51, p. 65-133, nov. 2017b.

BURRI, Mira. Understanding and Shaping Trade Rules for the Digital Era. In: ELSIG, M.; HAHN, M.; SPILKER, G. (eds.). **The Shifting Landscape of Global Trade Governanc**e: World Trade Forum. Cambridge: Cambridge University Press, 2019, p. 73-106.

BYGRAVE, Lee A. Data privacy law and the Internet: Policy challenges. In: WITZLEB, N. et al (eds.). **Emerging Challenges in Privacy Law**: Comparative Perspectives. Cambridge: Cambridge University Press, 2014, p. 259-289.

CASTELLS, Manuel. **A sociedade em rede**. 17 ed rev e amp. São Paulo: Paz e Terra, 2016.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Zahar, 2003. Edição do Kindle.

CASALINI, F.; GONZÁLES, J. López. Trade and Cross-Border Data Flows. **OECD Trade Policy Papers**, n. 220. OECD Publishing: Paris, 2019. Disponível em: http://dx.doi.org/10.1787/b2023a47-en. Acesso em: 21 nov. 2019.

CHANDER, Anupam. National Data Governance in a Global Economy. In: **UC Davis Legal Studies Research Paper**, n. 495, abr. 2016. Disponível em: https://ssrn.com/abstract=2770053. Acesso em 17 jul. 2019.

CIURIAK, Dan; PTASHKINA, Maria. **The digital transformation and the transformation of the international trade**. RTA Exchange. Genebra: International Centre for Trade and Sustainable Development (ICTSD) e Inter-American Development Bank (IDB), 2018. Disponível em: www.rtaexchange.org. Acesso em: 26 jun. 2019.

CLIFFORD, Damian; AUSLOOS, Jef. Data Protection and the Role of Fairness. In: **Yearbook of European Law**, v. 37, p. 130-187, 2018.

CLOSS, Karla Fonseca. **Investimentos estrangeiros**: regulamentação internacional e acordos bilaterais. Curitiba: Juruá, 2010.

COHEN, Julie E. What privacy is for. In: **Harvard Law Review**, v. 126, p. 1904-1933, 2013.

COLANGELO, Giuseppe; MAGGIOLINO, Mariateresa. Data accumulation and the privacy-antitrust interface: insights from the Facebook case. In: **International Data Privacy Law**, v. 8, n. 3, p. 224-239, ago. 2018.

COLANGELO, Giuseppe, MAGGIOLINO, Mariateresa. Data Protection in Attention Markets: Protecting Privacy through Competition? In: **Journal of European Competition Law & Practice**, v. 8, n. 6, p. 363-369, jun. 2017.

COLONNA, Liane. Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbor Program? In: **International Data Privacy Law**, v. 4, n. 3, p. 203-221, ago. 2014.

CORY, Nigel. **Cross-border data flows**: where are the barriers, and what do they cost? Maio/2017. Disponível em: http://www2.itif.org/2017-cross-border-data-

flows.pdf?_ga=2.199143599.1632613222.1563488057-528623298.1557188477. Acesso em: 18 jul. 2019.

COSTA, Cynara de Barros. **Direito Transnacional do Comércio**: Uma teoria afirmativa da natureza jurídica das normas do comércio internacional. 2016. 262 f. Tese (Doutorado em Direito). Programa de Pós-Graduação em Direito, Centro de Ciências Jurídicas / Faculdade de Direito do Recife, Universidade Federal de Pernambuco, Recife, 2016.

COSTA, José Augusto Fontoura. **Direito Internacional do investimento estrangeiro**. Curitiba: Juruá, 2010.

COSTA, José Augusto Fontoura. Aspectos geopolíticos do GATT e da OMC. **In: Revista de Direito Internacional**, v. 10, n. 1, p. 28-41, 2013.

CROSBY, Daniel. **Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments**. E15Initiative. Genebra: International Centre for Trade and Sustainable Development (ICTSD) e World Economic Forum, 2016. Disponível em: www.e15initiative.org/. Acesso em: 01 jun. 2019.

DAVEY, William. The WTO: Looking Forwards. In: **Journal of International Economic Law**, v. 9, n. 1, p. 3-29, mar. 2006.

DAVILLA, Marixenia. Is Big Data a Different Kind of Animal? The Treatment of Big Data Under the EU Competition Rules. In: **Journal of European Competition Law & Practice**, v. 8, n. 6, p. 370-381, jun. 2017.

D'CUNHA, Christian. Best of frenemies? Reflections on privacy and competition four years after the EDPS Preliminary Opinion. In: **International Data Privacy Law**, v. 8, n. 3, p. 253-257, ago. 2018.

DE BUSSER, Els. Adequate Transatlantic Data Exchange in the Shadow of the NSA-Affair. In: MILLER, R. (ed.). **Privacy and Power**: A Transatlantic Dialogue in the Shadow of the NSA-Affair. Cambridge: Cambridge University Press, 2017, p. 615-640.

DELIMATSIS, Panagiotis. Don't gamble with GATS - The Interaction between Articles VI, XVI, XVII and XVIII GATS in the light of the US - Gambling Case. In: **Journal of World Trade**, v. 40, n. 6, p. 1059-1080, 2006.

DETERMANN, Lothar. Adequacy of data protection in the USA: myths and facts. In: **International Data Privacy Law**, v. 6, n. 3, p. 244-250, ago. 2016.

DIAS, Bernadete de Figueiredo. **Investimentos estrangeiros no Brasil e o direito internacional**. Curitiba, Juruá, 2010.

DOCKSEY, Christopher. Four fundamental rights: finding the balance. In: **International Data Privacy Law**, v. 6, n. 3, p. 195-209, ago. 2016.

DU, Ming. The Necessity Test in World Trade Law: What Now? In: **Chinese Journal of International Law**, v. 15, n. 4, p. 817-847, dez. 2016.

ERDOS, David. Intermediary publishers and European data protection: Delimiting the ambit of responsibility for third-party rights through a synthetic interpretation of the EU acquis. In: **International Journal of Law and Information Tec**hnology, v. 26, n. 3, p. 189-225, 2018.

ESAYAS, Samson Y. Competition in (data) privacy: 'zero'-price markets, market power, and the role of competition law. In: **International Data Privacy Law**, v. 8, n. 3, p. 181-199, ago. 2018.

ESTEVE, Asunción. The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. In: **International Data Privacy Law**, v. 7, n. 1, p. 36-47, fev. 2017.

EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (ECIPE). **The Economic Importance of Getting Data Protection Right**: Protecting Privacy, Transmitting Data, Moving Commerce (2013). Disponível em: https:// www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf. Acesso em 02 jan. 2020.

EUROPEAN CENTRE FOR INTERNATIONAL POLITICAL ECONOMY (ECIPE). **The Costs of Data Localisation**: Friendly Fire on Economic Recovery (2014),. Disponível em: http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf. Acesso em: 02 jan. 2020.

FINCK, Michèle. Blockchains and the General Data Protection Regulation. In: **Blockchain Regulation and Governance in Europe**. Cambridge: Cambridge University Press, 2018, p. 88-116.

FLETT, James. WTO Space for National Regulation: Requiem for a Diagonal Vector Test. In **Journal of International Economic Law**, v. 16, n. 1, p. 37-90, mar. 2013.

FONG, Adrian. The role of app intermediaries in protecting data privacy. In: **International Journal of Law and Information Technology**, v. 25, n. 2, p. 85-114, 2017.

FRANTZIOU, Eleni. Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos. In: **Human Rights Law Review**, v. 14, n. 4, p. 761-777, dez. 2014.

GAMA JR., Lauro. **Contratos internacionais à luz dos princípios do UNIDROIT 2004**: *softlaw*, arbitragem e jurisdição. Rio de Janeiro: Renovar, 2006.

GAO, Henry. Digital or Trade? The Contrasting Approaches of China and US to Digital Trade. In: **Journal of International Economic Law**, v. 21, n. 2, p. 297-321, jun. 2018.

GARI, Gabriel. Is the WTO's Approach to International Standards on Services Outdated? In: **Journal of International Economic Law**, v. 19, n. 3, p. 589-605, 2016.

GASSER, Urs. Recoding Privacy Law: Reflections on the Future Relationship Among Law, Technology, and Privacy. In: **Harvard Law Review**, v. 130, n. 2, p. 61-70, 2016.

GONZÁLES, Javier López; JOUANJEAN, Marie-Anges. Digital trade: developing a framework for analysis. **OECD Trade Policy Papers**, n. 205, 2017. Paris: OECD Publishing. Disponível em: http://dx.doi.org/10.1787/524c8c83-en. Acesso em 26 jun. 2019.

GONZÁLES, Javier López; FERENCZ, Janos. Digital Trade and Market Openness. **OECD Trade Policy Papers**, n. 217, 2018. Paris: OECD Publishing. Disponível em: http://dx.doi.org/10.1787/1bd89c9a-en. Acesso em 25 jun. 2019.

GREENBERG, Marc H. A Return to Lilliput: The LICRA v. Yahoo - Case and the Regulation of Online Content in the World Market. In: **Berkeley Technology Law Journal**, v. 18, p. 1191-1258, 2003.

GREENLEAF, Graham. The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. In: **International Data Privacy Law**, v. 2, n. 2, p. 68-92, maio 2012.

GREENLEAF, Graham. A world data privacy treaty? “Globalisation” and “modernisation” of Council of Europe Convention 108. In: WITZLEB, N. et al (eds.). **Emerging Challenges in Privacy Law**: Comparative Perspectives. Cambridge: Cambridge University Press, 2014, p. 92-138.

GREENLEAF, Graham. Free Trade Agreements and Data Privacy: Future Perils of Faustian Bargains. In: SVANTESSON, D.; KLOZA, D. (eds.). **Trans-Atlantic Data Privacy Relations as a Challenge for Democracy**. Cambridge: Intersentia, 2017, pp. 181-212.

GREER, Damon. Safe Harbor - a framework that works. In: **International Data Privacy Law**, v. 1, n. 3, p. 143-148, ago. 2011.

GREZE, Benjamin. The extra-territorial enforcement of the GDPR: a genuine issue and the quest for alternatives. In: **International Data Privacy Law**, v. 9, n. 2, p. 109-128, maio 2019.

GUNASEKARA, Gehan. The “Final” Privacy Frontier? Regulating Trans-Border Data Flows. In: **International Journal of Law and Information Technology**, v. 17, n. 2, p. 147-179, 2009.

GUNASEKARA, Gehan. Paddling in unison or just paddling? International trends in reforming information privacy law. In: **International Journal of Law and Information Technology**, v. 22, n. 2, p. 141-177, 2014.

HERMAN, Lior. Multilateralising regionalism: the case of e-commerce. **OECD Trade Policy Papers**, n. 99. OECD Publishing: Paris. Disponível em: http://dx.doi.org/10.1787/5kmbjx6gw69x-en. Acesso em: 17 maio 2019.

HERT, Paul de; CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. In: **International Data Privacy Law**, v. 6, n. 3, p. 230-243, ago. 2016.

HODSON, Susannah. Applying WTO and FTA Disciplines to Data Localization Measures. In: **World Trade Review**, p. 1-29, 2018.

HOEKMAN, Bernard. Fostering Transatlantic Regulatory Cooperation and Gradual Multilateralization. In: **Journal of International Economic Law**, v. 18, n. 3, p. 609-624, set. 2015.

HON, W. Kuan et al. Policy, legal and regulatory implications of a Europe-only cloud. In: International Journal of Law and Information Technology, v. 24, n. 3, p. 251-278, 2016.

HONDIUS, Fritz. A Decade of International Data Protection. In: **Netherlands International Law Review**, v. 30, n. 2, p. 103-128, 1983.

HUANG, Zhixiong; MAČÁK, Kubo. Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches. In: **Chinese Journal of International Law**, v. 16, n. 2, p. 271-310, jun. 2017.

HUFBAUER, Gary Clyde; CIMINO-ISAACS, Cathleen. How will TPP and TTIP Change the WTO System? In: **Journal of International Economic Law**, v. 18, n. 3, p. 679-696, set. 2015.

HUSTINX, Peter. The reform of EU data protection: Towards more effective and more consistent data protection across the EU. In: WITZLEB, N. et al (eds.). **Emerging Challenges in Privacy Law**: Comparative Perspectives. Cambridge: Cambridge University Press, 2014, p. 62-72.

HYESY, Lee. **Data protection of digital trade and trade agreements**: concentrating on EU's legal development. 2018. 73 f. Dissertação (Mestrado). Graduate School of International Studies. Seoul National University, Seoul, Coréia do Sul, 2018.

INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITIC). **The EU-U.S. Privacy Shield: What's at Stake** (2016). Disponível em: http://www.itic.org/dotAsset/9/b/9b4cb3ad-6d8b-469d-bd03-b2e52d7a0ecd.pdf. Acesso em: 10 jan. 2020.

JAREMBA, Urszula; LALIKOVA, Laura. Effectiveness of Private Enforcement of European Competition Law in Case of Passing-on of Overcharges: Implementation of

Antitrust Damages Directive in Germany, France, and Ireland. In: **Journal of European Competition Law & Practice**, v. 9, n. 4, p. 226-236, abr. 2018.

KHAN, Lina. Amazon's antitrust paradox. In: **Yale Law Journal**, v. 126, n. 3, 2016-2017, p. 712-805.

KELSEY, Jane. How a TPP-Style E-commerce Outcome in the WTO would Endanger the Development Dimension of the GATS Acquis (and Potentially the WTO). In: **Journal of International Economic Law**, v. 21, n. 2, p. 273-295, jun. 2018.

KERBER, Wolfgang. Digital markets, data, and privacy: competition law, consumer law and data protection. In: **Journal of Intellectual Property Law & Practice**, v. 11, n. 11, p. 856-866, dez. 2016.

KIMMELMAN, Eugene; FELD, Harold; ROSSI, Agustín. The limits of antitrust in privacy protection. In: **International Data Privacy Law**, v. 8, n. 3, p. 270-276, ago. 2018.

KIRBY, Michael. The history, achievement and future of the 1980 OECD guidelines on privacy. In: **International Data Privacy Law**, v. 1, n. 1, p. 6-14, fev. 2011.

KLOZA, Dariusz; MOŚCIBRODA, Anna. Making the case for enhanced enforcement cooperation between data protection authorities: insights from competition law. In: **International Data Privacy Law**, v. 4, n. 2, p. 120-138, maio 2014.

KO, Haksoo et al. Structure and enforcement of data privacy law in South Korea. In: **International Data Privacy Law**, v. 7, n. 2, p. 100-114, maio 2017.

KOBRIN, Stephen J. Safe harbours are hard to find: The trans-Atlantic data privacy dispute, territorial jurisdiction and global governance. In: **Review of International Studies**, v. 30, n. 1, p. 111-131, 2004.

KONG, Lingjie. Data Protection and Transborder Data Flow in the European and Global Context. In: **European Journal of International Law**, v. 21, n. 2, p. 441-456, maio 2010.

KONG, Lingjie. Enacting China's Data Protection Act. In: **International Journal of Law and Information Technology**, v. 18, n. 3, p. 197-226, 2010.

KORNBECK, Jacob. Transferring athletes' personal data from the EU to third countries for anti-doping purposes: applying Recital 112 GDPR in the post-Schrems era. In: **International Data Privacy Law**, v. 6, n. 4, p. 291-298, nov. 2016.

KRISTRINA, Irion; SVETLANA, Yakovleva; MARIJA, Bartl. **Trade and Privacy**: Complicated Bedfellows? How to Achieve Data Protection-Proof Free Trade Agreements. Julho/2016. Disponível em: http://dx.doi.org/10.2139/ssrn.2877166. Acesso em: 13 mar. 2019.

KULESZA, Joanna. International law challenges to location privacy protection. In: **International Data Privacy Law**, v. 3, n. 3, p. 158-169, ago. 2013.

KUNER, Christopher. Data Protection Law and International Jurisdiction on the Internet (Part 1). In: **International Journal of Law and Information Technology**, v. 18, n. 2, p. 176-193, 2010.

KUNER, Christopher. Data Protection Law and International Jurisdiction on the Internet (Part 2). In: **International Journal of Law and Information Technology**, v. 18, n. 3, p. 227-247, 2010.

KUNER, Christopher. **Transborder Data Flows and Data Privacy Law**. OUP Oxford, 2013. Edição do Kindle.

KUNER, Christopher. Extraterritoriality and regulation of international data transfers in EU data protection law. In: **International Data Privacy Law**, v. 5, n. 4, p. 235-245, nov. 2015.

KÜZECI, Elif; BOZ, Beril. The new Data Protection Act in Turkey and its potential implication for E-commerce. In: **International Data Privacy Law**, v. 7, n. 3, p. 219-230, ago. 2017.

LANCIERI, Filippo Maria. Digital protectionism? Antitrust, data protection, and the EU/US transatlantic rift. In: **Journal of Antitrust Enforcement**, v. 7, n. 1, p. 27-53, mar. 2019.

LESIEUR, François. Regulating cross-border data flows and privacy in the networked digital environment and global knowledge economy. In: **International Data Privacy Law**, v. 2, n. 2, p. 93-104, maio 2012.

LEVIATHAN SECURITY GROUP. **Quantifying the Cost of Forced Localization** (2015). Disponível em: https://www.leviathansecurity.com/blog/quantifying-the-cost-of-forced-localization. Acesso em: 03 jan. 2020.

LEVIN, Avner; NICHOLSON, Mary Jo. Privacy Law in the United States, the EU and Canada: the allure of the middle ground. In: **University of Ottawa Law & Technology Journal**, v. 2, n. 2, p. 357-395, 2005.

LINDSAY, David. The Role of Proportionality in Assessing Trans-Atlantic Flows of Personal Data. In: SVANTESSON, D.; KLOZA, D. (eds.). **Trans-Atlantic Data Privacy Relations as a Challenge for Democracy**. Cambridge: Intersentia, 2017, p. 49-84.

LIU, Han-Wei. Data Localization and Digital Trade Barriers: ASEAN in Megaregionalism. In: HSIEH, P.; MERCURIO, B. (eds.). **ASEAN Law in the New Regional Economic Order**: Global Trends and Shifting Paradigms. Cambridge: Cambridge University Press, 2019, p. 371-391.

LUCCHINI, Stefano et al. Online Digital Services and Competition Law: Why Competition Authorities Should be More Concerned About Portability Rather than About Privacy. In: **Journal of European Competition Law & Practice**, v. 9, n. 9, p. 563-568, nov. 2018.

LUND, Susan; MANYIKA, James. **How digital trade is transforming glob**alisation. E15Initiative. Genebra: International Centre for Trade and Sustainable Development (ICTSD) e World Economic Forum (IDB), 2016. Disponível em: www.e15initiative.org. Acesso em: 29 jun. 2019.

LYNSKEY, Orla. The "Europeanisation" of Data Protection Law. In: **Cambridge Yearbook of European Legal Studies**, v. 19, p. 252-286, 2017.

MAIER, Bernhard. How Has the Law Attempted to Tackle the Borderless Nature of the Internet? In: **International Journal of Law and Information Technology**, v. 18, n. 2, p. 142-175, 2010.

MAKULILO, Alex Boniface. Privacy and data protection in Africa: a state of the art. In: **International Data Privacy Law**, v. 2, n. 3, p. 163-178, ago. 2012.

MARCHETTI, Juan; MAVROIDIS, Petros. The Genesis of the GATS (General Agreement on Trade in Services). In: **European Journal of International Law**, v. 22, n. 3, p. 689-721, ago. 2011.

MAKULILO, Alex Boniface. Data Protection Regimes in Africa: too far from the European "adequacy" standard? In: **International Data Privacy Law**, v. 3, n. 1, p. 42-50, fev. 2013.

MANDEL, Michael. **The Economic Impact of data:** Why data is not like oil (2017). Disponível em: https://www.progressivepolicy.org/publications/economic-impact-data-data-not-like-oil/. Acesso em: 01 dez. 2019.

MANTELERO, Alessandro. Competitive value of data protection: the impact of data protection regulation on online behaviour. In: **International Data Privacy Law**, v. 3, n. 4, p. 229-238, nov. 2013.

MARSOOF, Althaf. A case for sui generis treatment of software under the WTO regime. In: **International Journal of Law and Information Technology**, v. 20, n. 4, p. 291-311, 2012.

MAYER-SCHÖNBERGER, Viktor; RAMGE, Thomas. **Reinventing capitalism in the age of big data**. Nova York: Basic Books, 2018. Edição do Kindle.

MCQUINN, Alan; CASTRO, Daniel. **How law enforcement should access data across borders**. Jul./2017. Disponível em: https://itif.org/publications/2017/07/24/how-law-enforcement-should-access-data-across-borders. Acesso em: 18 jul. 2019.

MCCULLAGH, Karen. Brexit: potential trade and data implications for digital and fintech industries. In: **International Data Privacy Law**, v. 7, n. 1, p. 3-21, fev. 2017.

MCGILLIVRAY, Kevin. A right too far? Requiring cloud service providers to deliver adequate data security to consumers. In: I**nternational Journal of Law and Information Technology**, v. 25, n. 1, p. 1-25, 2017.

MCKINSEY GLOBAL INSTITUTE (MGI). Digital globalization: the new era of global flows (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.ashx. Acesso em: 20 jun. 2018.

MELTZER, Joshua Paul. **A new digital trade agenda**. E15Initiative. Genebra: International Centre for Trade and Sustainable Development (ICTSD) e World Economic Fotum (IDB), 2015. Disponível em: www.e15initiative.org. Acesso em 29 jun. 2019.

MELTZER, Joshua Paul. The internet, cross-border data flows and international trade. In: **Asia & Pacific Policy** Studies, v. 2, n. 1, p. 90-102, 2015.

MELTZER, Joshua Paul. **Maximizing the opportunities of the internet for international trade**. E15 Expert Group on the Digital Economy – Policy Option Paper. E15Initiative. Genebra: International Centre for Trade and Sustainable Development (ICTSD) e World Economic Fotum (IDB), 2016. Disponível em: www.e15initiative.org. Acesso em: 28 jun. 2019.

MELTZER, Joshua Paul; LOVELOCK, Peter. Regulating for a digital economy: understanding the importance of cross-border data flows in Asia. **Global Economy & Development Working Paper 113**, mar.2018. Disponível em: https://www.brookings.edu/wp-content/uploads/2018/03/digital-economy_meltzer_lovelock_web.pdf. Acesso em: 16 jul. 2019.

MELTZER, Joshua Paul; MATTOO, Aaditya. International data flows and privacy: the conflict and its resolution. In: **Journal of International Economic Law**, v. 21, n. 4, p. 769-789, dez. 2018.

MISHRA, Neha. The Role of the Trans-Pacific Partnership Agreement In the Internet Ecosystem: Uneasy Liaison or Synergistic Alliance? In: **Journal of International Economic Law**, v. 20, n. 1, p. 31-60, mar. 2017.

MITCHELL, Andrew D.; NERA, Mishra. Data at the docks: modernising International Trade Law for the digital economy. In: **Vanderbilt Journal of Entertainment & Technology Law**, v. 20, p. 1073-1134, 2018.

MITCHELL, Andrew D.; NERA, Mishra. Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute. In: **Journal of International Economic Law**, v. 22, n 3, p 389-416, set. 2019.

MOEREL, Lokke. The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? In: **International Data Privacy Law**, v. 1, n. 1, p. 28-46, fev. 2011.

MOEREL, Lokke. Back to basics: when does EU data protection law apply? In: **International Data Privacy Law**, v. 1, n. 2, p. 92-110, maio 2011.

MURPHY, Thérèse; CUINN, Gearóid Ó. Works in Progress: New Technologies and the European Court of Human Rights. In: **Human Rights Law Review**, v. 10, n. 4, p. 601-638, dez. 2010.

MURPHY, Thérèse; HEPBURN, Jarrod. Don't fence me in: reforming Trade and Investment Law to better facilitate cross-border data transfer. In: **Yale Journal of Law and Technology**, v. 19, p. 182-237, 2017.

MURPHY, Sean. U. S. EU “Safe Harbor” Data Privacy Arrangement. In: **American Journal of International Law**, v. 95, n. 1, p. 156-159, 2001.

MURRAY, Andrew D. Data transfers between the EU and UK post Brexit? In: **International Data Privacy Law**, v. 7, n. 3, p. 149-164, 2017.

NANDA, Ved P. The Communication Revolution and the Free Flow of Information in a Transnational Setting. In: **The American Journal of Comparative Law**, v. 30, p. 411-425, 1982.

NEUWIRTH, Rostam J. Global Market Integration and the Creative Economy: The Paradox of Industry Convergence and Regulatory Divergence. In: **Journal of International Economic Law**, v. 18, n. 1, p. 21-50, mar. 2015.

OBERGFELL, Eva Inés; THAMER, Alexander. (Non-)regulation of online platforms and internet intermediaries – the facts: Context and overview of the state of play. In: **Journal of Intellectual Property Law & Practice**, v. 12, n. 5, p. 435-441, maio 2017.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OCDE). **OECD Digital Economy Outlook 2017**. Disponível em: https://www.oecd-ilibrary.org/deliver/9789264276284-en.pdf?itemId=/content/publication/9789264276284-en&mimeType=application/pdf. Acesso em: 19 ago. 2018.

PADOVA, Yann. The Safe Harbour is invalid: what tools remain for data transfers and what comes next? In: **International Data Privacy Law**, v. 6, n. 2, p. 139-161, maio 2016.

PASQUALE, Frank A. Privacy, Antitrust, and Power. In: **George Mason Law Review**, v. 20, n. 4, p. 1009-1024, 2013.

PAUWELYN, Joost H. B. The Transformation of World Trade. In: **Michigan Law Review**, v. 104, n. 1, p. 1-66, 2005.

PENG, Shin-yi. GATS and the Over-the-Top Services: A Legal Outlook. In: **Journal of World Trade**, v. 50, n. 1, p. 21-46, fev. 2016.

PETKOVA, Bilyana. Domesticating the “foreign” in making transatlantic data privacy law. In: **International Journal of Constitutional Law**, v. 15, n. 4, p. 1135-1156, out. 2017.

PIETRZAK, Sylwia. Transborder data flows: binding corporate rules as a global transfer mechanism and trusted data processing area. 2017. 66 f. Dissertação (Mestrado). Tilburg University. Tilurg, Holanda, 2017.

POSCHER, Ralf. The Right to Data Protection. In: MILLER, Russel (ed.). **Privacy and Power**: A Transatlantic Dialogue in the Shadow of the NSA-Affair. Cambridge: Cambridge University Press, 2017, p. 129-142.

POLČÁK, Radim. Getting European data protection off the ground. In: **International Data Privacy Law**, v. 4, n. 4, p. 282-289, nov. 2014.

PORGES, Amy; ENDERS, Alice. **Data moving across borders**: the future of digital trade policy. E15Initiative. Genebra: International Centre for Trade and Sustainable Development (ICTSD) e World Economic Fotum (IDB), 2016. Disponível em: www.e15initiative.org. Acesso em: 28 jun. 2019.

POST, David. How the Internet is making jurisdiction sexy (again). In: **International Journal of Law and Information Technology**, v. 25, n. 4, p. 249-258, 2017.

PROUST, Olivier; BARTOLI, Emmanuelle. Binding Corporate Rules: a global solution for international data transfers. In: **International Data Privacy Law**, v. 2, n. 1, p. 35-39, fev. 2012.

QIN, Julia Ya. Pushing the Limits of Global Governance: Trading Rights, Censorship and WTO Jurisprudence - A Commentary on the China-Publications Case. In: **Chinese Journal of International Law**, v. 10, n. 2, p. 271-322, jun. 2011.

REDING, Viviane. The European data protection framework for the twenty-first century. In: **International Data Privacy Law**, v. 2, n. 3, p. 119-129, ago. 2012.

REYNA, Agustín. The psychology of privacy - what can Behavioural Economics contribute to competition in digital markets? In: **International Data Privacy Law**, v. 8, n. 3, p. 240-252, ago. 2018.

RODRIGUES, Rowena; WRIGHT, David; WADHWA, Kush. Developing a privacy seal scheme (that works). In: **International Data Privacy Law**, v. 3, n. 2, p. 100-116, maio 2013.

ROESSLER, Beate. Should personal data be a tradable good? On the moral limits of markets in privacy. In: ROESSLER, Beate; MOKROSINSKA, D. (eds.). **Social Dimensions of Privacy**: Interdisciplinary Perspectives. Cambridge: Cambridge University Press, 2015, p. 141-161.

ROSLER, Debra B. The European Union's proposed Directive for the legal protection of databases: a new threat to the free flow of information. In: **Berkeley Technology Law Journal**, v. 10, n. 1, p. 105-146, 1995.

ROSS, Alec. **The industries of the future**. Nova York: Simon & Schuster, 2016.
RUDDY, Brendan. The Critical Success of the WTO: Trade Policies of the Current Economic Crisis. In: **Journal of International Economic Law**, v. 13, n. 2, p. 475-495, jun. 2010.

RUSTAD, Michael L.; KULEVSKA, Sanna. Reconceptualizing the right to be forgotten to enable transatlantic data flow. In: **Harvard Journal of Law and Technology**, v. 28, n. 2, 349-417, 2015.

SAUVÉ, Pierre. To fuse, Not to Fuse, or Simply Confuse? Assessing the Case for Normative Convergence Between Goods and Services Trade Law. In: **Journal of International Economic Law**, v. 22, n 3, p 355-371, set. 2019.

SAVAGE, N.; EDWARDS, C. Transborder Data Flows: The European Convention and United Kingdom Legislation. In: **International and Comparative Law Quarterly**, v. 35, n. 3, p. 710-717, 1986.

SCHARTUM, Dag Wiese. Designing and Formulating Data Protection Laws. In: **International Journal of Law and Information Technology**, v. 18, n. 1, p. 1-27, 2010.

SCHMITT, Michael; WATTS, Sean. Beyond State-Centrism: International Law and Non-state Actors in Cyberspace. In: **Journal of Conflict and Security Law**, v. 21, n. 3, p. 595-611, 2016.

SCHNEIDER, Giulia. Testing Art. 102 TFEU in the Digital Marketplace: Insights from the Bundeskartellamt's investigation against Facebook. In: **Journal of European Competition Law & Practice**, v. 9, n. 4, p. 213-225, abr. 2018.

SCHWAB, Klaus. **The fourth industrial revolution**. Nova York: Crown Business, 2017. Edição do Kindle.

SCHWARTZ, Paul M; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. In: **New York University Law Review**, v. 86, p. 1814-1893, 2011.

SCHWARTZ, Paul M. The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. In: **Harvard Law Review**, v. 126, p.1966-2009, maio 2013.

SCHWARTZ, Paul M; SOLOVE, Daniel J. Reconciling Personal Information in the United States and European Union. In: **California Law Review**, v. 102, p. 877-916, 2014.

SCHWARTZ, Paul M.; PEIFER, Karl-Nikolaus. Transatlantic Data Privacy Law. In: **The Georgetown Law Journal**, v. 106, n. 115, p. 115-179, nov. 2017.

SCHWEIGHOFER, Erich. Principles for US-EU Data Flow Arrangements. In: SVANTESSON, D.; KLOZA, D. (eds.). **Trans-Atlantic Data Privacy Relations as a Challenge for Democracy**. Cambridge: Intersentia, 2017, p. 27-48.

SELBY, John. Data localization laws: trader barriers or legitimate responses to cybersecurity risks, or both? In: **International Journal of Law and Information Technology**, v. 25, n. 3, p. 213-232, jul. 2017.

SEN, Nivedita. Understanding the role of the WTO in international data flows: taking the liberalization or the regulatory autonomy path? In: **Journal of International Economic Law**, v. 21, n. 2, p. 323-348, jun. 2018.

SHAFFER, Gregory. Extraterritoriality in a Globalizing World: Regulation of Data Privacy. In: **Proceedings of the ASIL Annual Meeting**, v. 97, p. 314-317, abr. 2003.

SILVA, Alice Rocha da; SOARES, Filipe Rocha Martins. Conflitos entre regulações internas relativas à internet e o direito do comércio internacional: o papel da OMC perante o sistema de computação da nuvem. In: **Revista de Direito Internacional**, v. 14, n. 1, p. 238-247, 2017.

SLOKENBERGA, Santa et al. EU data transfer rules and African legal realities: is data exchange for biobank research realistic? In: **International Data Privacy Law**, v. 9, n. 1, p. 30-48, fev. 2019.

SOLOVE, Daniel J. A taxonomy of privacy. In: **University of Pennsylvania Law Review**, v. 154, n. 3, p. 477-560, jan. 2006.

SOKOL, Daniel; COMERFORD, Roisin. Does Antitrust Have a Role to Play in Regulating Big Data? In: BLAIR, R.; SOKOL, Daniel (eds.). **The Cambridge Handbook of Antitrust, Intellectual Property, and High Tech**. Cambridge: Cambridge University Press, 2017, p. 293-316.

SORIEUL, Renaud. Brief overview of international initiatives for an electronic commerce uniform legal framework. In: **Uniform Law Review**, v. 4, n. 4, p. 908-927, 1999.

STALLWORTHY, M. Data Protection: Regulation in a Deregulatory State. In: **Statute Law Review**, v. 11, n. 2, p. 130-154, 1990.

STREATFIELD, Christine M. Personal data privacy and the WTO. In: **Houston Journal of International Law**, v. 36, n. 3, p. 625-652, 2014.

SVANTESSON, Dan Jerker. The regulation of cross-border data flows. In: **International Data Privacy Law**, v. 1, n. 3, p. 180-198, ago. 2011.

SVANTESSON, Dan Jerker. Extraterritoriality in the context of data privacy regulation. In: **Masaryk University Journal of Law and Technology**, v. 7, n.1, p. 87-96, 2012.

SVANTESSON, Dan Jerker. The holy trinity of legal fictions undermining the application of law to the global Internet. In: **International Journal of Law and Information Technology**, v. 23, n. 3, p. 219-234, 2015.

SVANTESSON, Dan. A legal method for solving issues of Internet regulation. In: **International Journal of Law and Information Technology**, v. 19, n. 3, p. 243-263, 2011.

TAVENGERWEI, Rutendo. Using Trade Facilitation to Assist MSMEs in E-Commerce in Developing Countries. In: **Journal of International Economic Law**, v. 21, n. 2, p. 349-378, jun. 2018.

TAYLOR, Mistale. The EU's human rights obligations in relation to its data protection laws with extraterritorial effect. In: **International Data Privacy Law**, v. 5, n. 4, p. 246-256, nov. 2015.

TENE, Omer. Privacy: The new generations. In: **International Data Privacy Law**, v. 1, n. 1, p. 15-27, fev. 2011.

TOURKOCHORITI, Ioanna. The Transatlantic Flow of Data and the National Security Exception in the European Data Privacy Regulation: In Search for Legal Protection Against Surveillance. In: **University of Pennsylvania Journal of International Law**, v. 36, p. 459-524, 2014.

TZANOU, Maria. European Union Regulation of Transatlantic Data Transfers and Online Surveillance. In: **Human Rights Law Review**, v. 17, n. 3, p. 545-565, set. 2017.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). **Information Economy Study 2015 - Unlocking the Potential of E-commerce for Developing countries** (2015). Disponível em: http://unctad.org/en/PublicationsLibrary/ier2015_ en.pdf. Acesso em: 12 jan. 2020.

UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT (UNCTAD). **Data protection regulations and international data flows**: implications for trade and development (2016). Disponível em: https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf. Acesso em: 18 jul. 2019.

VAN ALSENOY, Brendan. Scope of EU Data Protection Law. In: **Data Protection Law in the EU**: Roles, Responsibilities and Liability. Cambridge: Intersentia, 2019, p. 25-32.

VAN ALSENOY, Brendan. The Emergence of Data Protection Law. In: **Data Protection Law in the EU**: Roles, Responsibilities and Liability. Cambridge: Intersentia, 2019, p. 155-162.

VAN ALSENOY, Brendan. National Data Protection Laws before 1980. In: **Data Protection Law in the EU**: Roles, Responsibilities and Liability. Cambridge: Intersentia, 2019, p. 163-206.

VAN ALSENOY, Brendan. International Instruments. In: **Data Protection Law in the EU**: Roles, Responsibilities and Liability. Cambridge: Intersentia, 2019, p. 207-230.

VAN ALSENOY, Brendan. National Data Protection Laws after 1981. In: **Data Protection Law in the EU**: Roles, Responsibilities and Liability. Cambridge: Intersentia, 2019, p. 231-260.

VAN DEN HOVEN, Jeroen. Information Technology, Privacy, and the Protection of Personal Data. In: VAN DEN HOVEN, Jeroen; WECKERT, J. (eds.). **Information Technology and Moral Philosophy**. Cambridge: Cambridge University Press, 2008, p. 301-321.

VAN DER SLOOT, Bart. Do data protection rules protect the individual and should they? An assessment of the proposed General Data Protection Regulation. In: **International Data Privacy Law**, v. 4, n. 4, p. 307-325, nov. 2014.

VAN DER SLOOT, Bart. The Transformation of the Right to Privacy and the Right to Data Protection. In: **Privacy as Virtue**: Moving Beyond the Individual in the Age of Big Data. Cambridge: Intersentia, 2017, p. 11-70.

VICENTE, Dário Moura. **Direito Comparado** – V. 1: introdução e parte geral. Coimbra: Almedina, 2008.

VICTOR, Jacob. The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy. In: **Yale Law Journal**, v. 123, p. 513-528, 2013.

VOSS, W. Gregory. After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change. In: **Business Lawyer**, v. 71, n. 1, p. 281/292, 2016.

WEBER, Rolf. Digital Trade in WTO-Law - Taking Stock and Looking Ahead. In: **Asian Journal of WTO & International Health Law and Policy**, v. 5, n. 1, pp. 1-24, mar. 2010.

WEBER, Rolf. Regulatory Autonomy and Privacy Standards Under the GATS. In: **Asian Journal of WTO & International Health Law and Policy**, v. 7, n. 1, p. 25-48, mar. 2012.

WEBER, Rolf. Transborder data transfers: concepts, regulatory approaches and new legislative initiatives. In: **International Data Privacy Law**, v. 3, n. 2, p. 117-130, maio 2013.

WEBER, Rolf. Transnational Data Privacy in the EU Digital Single Market Strategy. In: SVANTESSON, D.; KLOZA, D. (eds.). **Trans-Atlantic Data Privacy Relations as a Challenge for Democracy**. Cambridge: Intersentia, 2017, p. 5-26.

WHITE, Alison. Control of Transborder Data Flow: Reactions to the European Data Protection Directive. In: **International Journal of Law and Information Technology**, v. 5, n. 2, p. 230-247, 1997.

WIEBE, Andreas. Data protection and the internet: irreconcilable opposites? The EU Data Protection Reform Package and CJEU case law. In: **Journal of Intellectual Property Law & Practice**, v. 10, n. 1, p. 64-68, jan. 2015.

WONG, Benjamin. Delimiting the concept of personal data after the GDPR. In: **Legal Studies**, v. 39, n. 3, p. 517-532, 2019.

WOJTAN, Boris. The new EU Model Clauses: One step forward, two steps back? In: **International Data Privacy Law**, v. 1, n. 1, p. 76-80, fev. 2011.

YAKOVLEVA, Svetlana. Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade “Deals”? In: **World Trade Review**, v. 17, n. 3, p. 477-508, 2018.

ZHANG, N. Trade Commitments and Data Flows: The National Security Wildcard: **Reconciling Passenger Name Record Transfer Agreements and European GATS Obligations**. In: World Trade Review, v. 18, n. 1, p. 49-62, 2019.

ZHAO, Bo; BONNICI, Jeanne Mifsud. Protecting EU citizens ’personal data in China: a reality or a fantasy? In: **International Journal of Law and Information Technology**, v. 24, n. 2, p. 128-150, 2016.