Fundação Getulio Vargas

Escola de Direito de São Paulo

FERNANDA MASCARENHAS MARQUES

REGULAÇÃO DO FLUXO DE DADOS PESSOAIS ENTRE FRONTEIRAS

Os contornos e limites da Decisão de Adequação de países terceiros

São Paulo

2020

FERNANDA MASCARENHAS MARQUES

REGULAÇÃO DO FLUXO DE DADOS PESSOAIS ENTRE FRONTEIRAS

Os contornos e limites da Decisão de Adequação de países terceiros

Dissertação apresentada à Escola de Direito de São Paulo da Fundação Getulio Vargas, como requisito para obtenção do título de Mestre em Direito e Desenvolvimento. Campo de conhecimento: Direito dos Negócios e Desenvolvimento Econômico e Social.

Orientador: Prof. Dr. Salem Hikmat Nasser

São Paulo

2020

Marques, Fernanda Mascarenhas
Regulação do fluxo de dados pessoais entre fronteiras: os contornos e limites da decisão de adequação de países terceiros / Fernanda Mascarenhas Marques. - 2020.
136f.

Orientador: Prof. Dr. Salem Hikmat Nasser
Dissertação (mestrado) – Fundação Getulio Vargas, Escola de Direito de São Paulo.

1. Proteção de dados - Legislação - Países da União Européia. 2. Direito à privacidade - Legislação. 3. Comissão Européia. 4. Conformidade. I. Nasser, Salem Hikmat. II. Dissertação (mestrado) - Escola de Direito de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 34::681.324

Ficha Catalográfica elaborada por: Isabele Oliveira dos Santos Garcia CRB SP-010191/O

Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

FERNANDA MASCARENHAS MARQUES

REGULAÇÃO DO FLUXO DE DADOS PESSOAIS ENTRE FRONTEIRAS

Os contornos e limites da Decisão de Adequação de países terceiros

Dissertação apresentada à Escola de Direito de São Paulo da Fundação Getulio Vargas, como requisito para obtenção do título de Mestre em Direito e Desenvolvimento. Campo de conhecimento: Direito dos Negócios e Desenvolvimento Econômico e Social.

Data de aprovação: ___/___/____

Prof. Dr. Salem Hikmat Nasser
Orientador, FGV Direito SP

Prof[a]. Dr[a]. Mônica Steffen Guise Rosina
FGV Direito SP

Prof. Dr. Marcel Leonardi
FGV Direito SP

Prof. Dr. Dennys Antonialli
Universidade de São Paulo - USP

À Therezinha, minha fonte de luz.

O presente trabalho foi realizado com apoio da Fundação Getúlio Vargas, por meio da bolsa Mario Henrique Simonsen de Ensino e Pesquisa.

Agradecimentos

Agradeço, em primeiro lugar, aos meus pais, Ana Alice e Renato, por serem desde sempre uma sustentação firme nessa caminhada em busca de conhecimento. Agradeço também meu companheiro de profissão e de vida, meu irmão Pedro.

Agradeço, nominalmente, com todo meu carinho, às quatro mulheres mais importantes da minha vida: minha mãe Ana Alice, pela demonstração diária de perseverança e dedicação; vovó There, por ter sido para mim a fonte mais bonita de luz e sabedoria; vovó Laila, pela demonstração genuína de força sobretudo nesses tempos sem vovô por perto; e Cristina, minha amiga que, antes de partir, me ensinou a força da busca pelo autoconhecimento.

Agradeço ao meu orientador Prof. Salem Hikmat Nasser e a todos os colegas, amigos, professores e funcionários da FGV-SP. Todas as trocas eu levo comigo e, com certeza, me serviram e continuarão servindo para novas reflexões acadêmicas. Agradeço, também nominalmente, ao Prof. José Garcez Ghirardi pelas palavras e reflexões ao longo deste processo. Agradeço à Bolsa Mario Henrique Simonsen pelo apoio para o desenvolvimento deste trabalho.

Agradeço aos amigos que fiz no Centro de Estudos do Comércio Global e Investimentos da FGV-EESP, sobretudo, pela oportunidade de poder trabalhar ao lado da Prof. Vera Thorstensen, a qual, com certeza, foi uma das grandes responsáveis por me fazer despertar para o mundo enorme que é o estudo dos temas relacionados ao comércio internacional. Agradeço também à parceria com Alexandre Coelho e à Giulia, amiga de pesquisa que o Centro me deu e, hoje, parceira de profissão.

Agradeço às minhas amigas de graduação da PUC-SP e, dentre elas, Samia Abdalla. Agradeço aos meus colegas que guardaram um pouco de tempo para ler, discutir e apontar sugestões para aprimoramento deste trabalho. Principalmente, ao Theofilo de Aquino, Maria Eugênia Kroetz, Magali Fernandes e Daniel Favoretto. Pelo cuidado com a formatação, agradeço ao Matheus Mascioli.

Agradeço ao Data Privacy Brasil, nomeadamente, ao Bruno Bioni, Renato Leite, Mariana Rielli e Fabiano Araújo pela oportunidade em fazer parte do time como monitora da Turma 6 e 7 do Curso de Extensão. A sala de aula sempre foi o lugar mais espontâneo e livre para reflexões acadêmicas. Com certeza, cada aula e cada debate contribuíram para que ideias surgissem ao longo da elaboração deste trabalho.

No mesmo sentido, agradeço à SBDP, por me propiciar experiência como professora convidada nas aulas de Jurisprudência Constitucional e como orientadora de monografias para conclusão do curso. Um especial obrigada ao Prof. Carlos Ari Sundfeld, Yasser Gabriel e Mariana Vilella.

Agradeço aos Profs. Dennys Antonialli e Alexandre Pacheco pelos comentários na banca de qualificação. Agradeço pelos comentários finais da Prof. Mônica Rosina, do Prof. Marcel Leonardi e Dennys Antonialli. Foram extremamente valiosos.

Por fim, agradeço também pela experiência e aos amigos do escritório Pereira Neto Macedo – PNM. Os meses de trabalho e a troca diária com os colegas me ajudaram a maturar o olhar sobre as sensibilidades que envolvem cada pequeno ponto dentro do direito de proteção dos dados pessoais. Meu especial obrigada à Equipe de Mídia, Tecnologia, Propriedade Intelectual e Proteção de Dados: Ronaldo Lemos, Daniel Douek, Natalia, Artur, Juliana, Sofia, Andrea, Leo, Giulia, Flavia, Gabriela e Isabela. Com certeza, uma pesquisadora só tem a ganhar com pessoas tão interessantes e qualificadas que encontra em seu caminho.

Resumo

Esta dissertação analisa as decisões de adequação proferidas pela Comissão Europeia sob as regras da Diretiva 95/46/CE e do atual *General Data Protection Regulation* (Regulamento nº 679/2016 ou GDPR). Para fazer isso, utiliza-se da categoria de análise desenvolvida por Graham Greenleaf que identifica a existência de dez padrões globais e dez padrões europeus de proteção de dados pessoais. Os dez padrões globais compreendem padrões comuns de proteção de dados pessoais contidos nas Diretrizes de 1980, Convenção 108, Diretiva 95/46/CE e APEC *Privacy Framework*. Por sua vez, os dez padrões europeus compreendem padrões típicos do regime regulatório europeu, encontrados, exclusivamente, na Convenção 108 e na Diretiva 95/46/CE. As decisões analisadas são apresentadas em três eixos distintos. O primeiro eixo compreende as decisões proferidas entre os anos de 2000 e 2012, ainda sob a Diretiva 95/46/CE (Suíça, Canadá, Guernsey, Argentina, Ilha de Man, Jersey, Andorra, Ilha Faroé, Israel, Nova Zelândia, Uruguai). O segundo compreende a decisão a respeito dos Estados Unidos, no âmbito de aplicação do *Privacy Shield*. Por fim, o terceiro eixo compreende a decisão do Japão, sendo a primeira proferida sob o atual regime do GDPR. A dissertação conclui que a União Europeia vem construindo um regime de regulação extraterritorial forte, em que se busca mecanismos capazes de proteger o nível adequado do tratamento dos dados pessoais independentemente do local de seu tratamento. As decisões, porém, demonstram uma análise superficial do regime jurídico do terceiro avaliado por parte da Comissão Europeia, bem como uma avaliação estática das regras de proteção dos dados pessoais.

Palavras-chave: transferência internacional. dados pessoais. decisão de adequação.

Abstract

This dissertation analysis the European Comission's adequacy decisions under the rules of the Directive 95/46/EC and the General Data Protection Regulation (GDPR or Regulation 2016/679). In order to so, it relies on Graham Greenleaf's categories of analysis, which identify the existence of ten global standards and ten European standards of data protection. The ten global standards comprise common standards of data protection contained in the Directives of 1980, the Convention 108, the Directive 95/46/EC, and the APEC Privacy Framework. The ten European standards, in turn, comprise standards that are typical of the European regulatory regime, found, exclusively, in the Convention 108 and in the Directive 95/46/EC. The analysed decisions are then presented in three distinct groups. The first group comprises the decisions rendered from 2000 and 2012, still under the Directive 65/46/EC ((Switzerland, Canada, Guernsey, Argentina, Isle of Man, Jersey, Andorra, Faroe Island, Israel, New Zealand, Uruguay). The second group comprises the decision on the United States with regards to the Privacy Shield Framework. Finally, the third group comprises the decision on Japan, the first decision rendered by the Commission under the current GDPR regime. This dissertation concludes that the European Union is setting up a strong regime of extraterritorial regulation, by which it searches for mechanisms that are capable of protecting an adequate level of data protection regardless of the place of its actual treatment. The decisions, however, demonstrate a superficial analysis of the legal regime of the third party under assessment, as well as a static assessment of the rules on data protection.

Keywords: international transfer. personal data. adequacy decision.

Lista de tabelas

Sumário

1 INTRODUÇÃO

1.1 Apresentação da pesquisa

Esta dissertação busca responder a seguinte pergunta: como decide a Comissão Europeia sobre os países reconhecidos com nível adequado de proteção de dados pessoais? Essa pergunta, conforme será desenvolvido ao longo desta dissertação, está inserida em um contexto macro em que se inserem diversos estudos que buscam compreender o fenômeno da harmonização de regras de proteção de dados pessoais em diversas jurisdições do globo. O Brasil, inclusive, passou a entrar na lista com a aprovação, em 2018, da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 ou LGPD).

A LGPD faz parte, portanto, de um movimento maior de proliferação de leis de proteção de dados pessoais em diversas jurisdições que incorporam denominadores comuns de proteção relacionados a certos conceitos, princípios e direitos dos titulares. Mais que isso, a sua aplicação segue a tendência de abranger atividades desenvolvidas pelos setores público e privado, sendo, ainda, neste último caso, aplicada transversalmente a todos os setores da economia. Por conta desta característica, a lei atrai sua denominação de "lei geral" de proteção de dados.

Esta dissertação está situada dentro deste contexto macro e busca contribuir para o tema da harmonização de regras de proteção de dados pessoais por meio da chave descritiva do desenvolvimento da regulação incidente sobre o fluxo transfronteiriço de dados pessoais. O desenvolvimento desta regulação levou ao então regime aqui estudado: o regime desenvolvido pela União Europeia desde 1995 por meio da Diretiva 95/46/CE, a qual criou o instituto sob análise nesta dissertação - a decisão de adequação. Trata-se, sucintamente, de um mecanismo destinado a avaliar sistemas jurídicos de países terceiros (não membros) e sua adequação em relação aos parâmetros europeus de proteção de dados pessoais, de forma a estabelecer um campo entre países em que se prepondera o livre fluxo de dados pessoais. Argumenta-se, ao longo desta dissertação, de que se trata de um instituto "motor" de propagação dos denominadores comuns de padrões europeus de proteção de dados a demais países do globo.

Estudar este campo é relevante uma vez que é por meio das preocupações extraterritoriais do tratamento dos dados pessoais que iniciativas regulatórias de harmonização de regras passaram a ser pensadas e adotadas por países, blocos econômicos ou organizações internacionais. A preocupação era de que, em conjunto com a necessidade de garantir a proteção da privacidade e dos dados pessoais, regulações protecionistas limitassem o comércio internacional, acabando por criar restrições ao fluxo de dados entre fronteiras e desvantagens no acesso ao mercado local de empresas estrangeiras.

Sobre isto, é possível ir além. De um lado, a harmonização levanta aspectos positivos

para o setor privado relacionados à diminuição dos custos de conformidade, sobretudo para os negócios digitais que nascem com a pretensão de atingir variadas jurisdições. Porém, os denominadores comuns podem também acabar por elevar o nível de exigência para a adequação e imputar custos às empresas locais não antes suportados. Nesse sentido, os denominadores comuns adotados por uma pluralidade de jurisdições diminuem incertezas aos negócios que se pretendem globais, mas, ao mesmo tempo, podem onerar a indústria e empresa local sem a devida participação esperada no processo de construção das regras. Diante disso, questiona-se, do ponto de vista interno, a respeito da importação de regras jurídicas sem a devida consideração às demandas e pautas locais, considerados fatores importantes no momento de formulação de regras, bem como a relevância de arranjos institucionais e jurídicos locais, que circunscrevem e delimitam as especificidades de um determinado país.

Esse dilema direciona o olhar para uma pluralidade de questionamentos, os quais não são objeto direto de resposta desta dissertação, mas estão, contudo, intrinsecamente ligados no desenvolvimento de cada etapa deste estudo. Em outras palavras, a harmonização de regras carrega consigo agentes e interesses específicos, os quais estão preocupados em estender influências para além do seu âmbito territorial original. Assim, questionamentos a respeito de quem são os agentes por trás da disseminação dessas regras e quais tipos de interesses defendem são fundamentais para compreensão do fenômeno estudado. Afinal, o processo de transplantes ou tradução normativos carrega consigo complexidades e dificuldades múltiplas, as quais estão relacionadas com toda uma bibliografia que busca evidenciar os problemas de importação e exportação de regras jurídicas.

Com isso em mente, esta dissertação contribui para o desenvolvimento dos seguintes temas (i) compreensão histórica da evolução da regulação do fluxo de dados pessoais entre fronteiras, que está diretamente relacionada ao desenvolvimento de denominadores comuns de proteção de dados; (ii) quais são os denominadores comuns de proteção de dados pessoais e quem são os principais agentes precursores e (iii) tradução e transplantes de normas jurídicas entre países, por meio de um mapeamento dos incentivos e institutos por trás dessa importação e exportação de regras – caso especifico estudado é o instituto da decisão de adequação, o qual entra como um dos fatores capazes de influenciar o processo de exportação de normas e regras jurídicas. A seguir, apresenta-se com mais detalhe a metodologia utilizada e os próximos capítulos desta dissertação.

1.2 Metodologia

Para auxiliar na condução desta análise, este estudo se propõe a analisar as decisões de adequação proferida pela Comissão Europeia desde a publicação da Diretiva 95/46/CE. As decisões foram proferidas entre os anos 2000 a 2019 e contam, atualmente, com o número de 13 decisões. A primeira delas foi proferida em relação à Suíça, no ano de 2000. A decisão da Suíça

foi seguida por Canada (2001), Guernsey (2003), Argentina, (2003), Ilha de Man (2004), Jersey (2008), Andorra (2010), Faroe Island (2010), Israel (2011), Nova Zelândia (2012), Uruguai (2012), Estados Unidos, no âmbito de proteção do *Privacy Shield* (2016), e, por fim, o Japão (2019).

O processo de leitura e exposição das decisões teve como fonte direta - mas não se restringiu a isto - trabalhos desenvolvidos por Greenleaf (2011, 2012a, 2012b, 2017, 2018), autor que possui publicações cujo escopo é focado na análise de legislações gerais de proteção de dados pessoais de diversos países e na compreensão de como cada legislação importou padrões de proteção de dados pessoais classificados como globais e europeus (ou ainda primeira e segunda geração de padrões de proteção de dados pessoais)[1].

Nessa linha, o autor busca sistematizar os denominadores comuns dos padrões de proteção vigentes em duas grandes chaves. Para chegar nesta sistematização, o autor analisou os padrões contidos nas Diretrizes da OCDE de 1980 e na APEC Framework de 2005 e comparou com aqueles contidos na Convenção 108 de 1981 (alterada pelo seu Protocolo Adicional em 2001) e na Diretiva 95/46/CE. A partir dessa comparação, o autor separou os padrões globais (não europeus) como sendo aqueles padrões que são compartilhados em todos os instrumentos normativos analisados e os padrões europeus como sendo aqueles padrões que somente estão previstos na Convenção 108 e/ou na Diretiva 95/46/EC[2].

A partir desta comparação normativa, o autor destaca dez padrões globais e dez padrões europeus de proteção de dados pessoais. Os padrões globais são vistos como o denominador mínimo comum de regras de proteção de dados pessoais (trata-se da chamada primeira geração), enquanto os padrões europeus apresentam critérios mais rígidos para as atividades de tratamento cujo objetivo é aumentar a proteção dos dados pessoais (chamada de segunda geração de proteção de dados pessoais).

Nesse sentido, em relação aos padrões globais de proteção de dados pessoais, os quais seriam, portanto, aqueles encontrados nas Diretrizes de 1980 da OCDE e na APEC Privacy Framework de 2005, Greenleaf destaca os seguintes[3]: (i) Limites na coleta, a qual deve ser

[1] "The term 'European standards' means standards required of European countries by the EU data protection Directive (1995) and by Council of Europe (CoE) data protection Convention 108 (1981) as modified by its Additional Protocol (2001), but which are not standards required by the '1st generation' standards of the OECD Guidelines (1980) and original CoE Convention 108 (1981). Put briefly, 'European' or '2nd generation' standards are the difference between what was required by the EU Directive as compared with the OECD. To be manageable, this has been limited to the ten most important differences, as set out in the attached Table."(GREENLEAF, 2017).

[2] "To argue that a law outside Europe is influenced by the EU Directive of 1995 (or the Council of Europe Convention), rather than by the preceding developments of the OECD Guidelines or the subsequent development of the APEC Privacy Framework, it is first necessary to identify two things (i) those elements which are shared between the Directive (and usually in Convention 108) and the OECD Guidelines; and (ii) those elements which are found in the Directive (and in some cases also in Convention 108) but are not required by the OECD Guidelines or the subsequent APEC Framework (in general, a weaker version of the OECD Guidelines). We can call the first 'global' elements and the second 'European' elements."(GREENLEAF, 2018).

[3] Os padrões são retirados do texto Greenleaf (2017, p. 7-8).

realizada por meios lícitos e justos, com consentimento ou conhecimento do titular de dados pessoais; (ii) Qualidade dos dados, os quais devem ser relevantes, precisos e atualizados; (iii) Finalidade específica no momento da coleta; (iv) Aviso da finalidade e dos direitos no momento da coleta; (v) Usos limitados, incluindo divulgações para fins específicos ou compatíveis; (vi) Segurança através de salvaguardas razoáveis; (vii) Transparência nas práticas de proteção de dados pessoais; (viii) Direito individual de acesso; (ix) Direito individual de correção e (x) *Accountability*, controladores de dados responsáveis pelas medidas de implementação das leis.

Sobre os padrões europeus de proteção de dados pessoais, estes ou amplificam o escopo de aplicação do primeiro ou criam ainda novos critérios necessários para obtenção de um regime adequado de proteção de dados pessoais, estes critérios constam somente na Convenção 108 e/ou na Diretiva 95/46/CE. Nesse sentido, Greenleaf cita: (i) Autoridade de proteção de dados independente; (ii) Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares; (iii) Restrição às exportações de dados pessoais para países que não possuem padrão adequado de proteção da privacidade; (iv) Minimização dos dados para a finalidade da coleta, não apenas limitada; (v) Tratamento lícito e justo (não só a coleta); (vi) Requisitos para a notificação e, às vezes, fornecimento de caixas de *check in* prévias para autorização de tipos específicos de tratamento de dados pessoais; (vii) Destruição ou anonimização de dados pessoais depois de um certo período; (viii) Proteções adicionais para categorias específicas de dados sensíveis; (ix) Limites na tomada de decisões automatizadas e o direito de conhecer a lógica do tratamento automatizado de dados pessoais; (x) Requisito para fornecer *opt-out* em casos de marketing direto de dados pessoais.

Esse padrão de proteção elevado advindo do modelo europeu também está relacionado à carga jurídico-valorativa dada ao direito de proteção dos dados pessoais na União Europeia, o qual é tutelado como direito fundamental, estabelecido no artigo 8º da Carta de Direitos Fundamentais da União Europeia - CDFUE[4]. Neste artigo, o direito à proteção dos dados pessoais é tutelado por meio de tratamento dos dados pessoais de forma justa e com finalidades específicas, mediante obtenção do consentimento do titular dos dados pessoais ou de outra base legítima estabelecida em lei. Ademais, todos os titulares dos dados pessoais têm o direito de acesso e retificação dos dados que foram coletados. A verificação de cumprimento dessas regras deve ocorrer por meio de uma autoridade independente.

Em síntese, padrões de regras de proteção de dados pessoais foram exportados às diversas legislações ao redor do mundo, esses padrões possuem origem em determinados instrumentos normativos que surgiram ao passar dos anos, são eles: (i) Diretrizes da OCDE, adotada pelo Conselho da OCDE em 1980; (ii) Convenção nº. 108, adotado em 1981 pelos membros do

[4] "Art. 8 – Protection of personal data 1.Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority."(UNIÃO EUROPEIA, 2000, art. 8).

Conselho da Europa e aberto para assinatura aos países não membros; (iii) Diretiva 95/46/EC, aprovada pelo Parlamento Europeu e o Conselho, em 1995, destinada à proteção dos indivíduos em relação ao tratamento dos dados pessoais e a livre circulação desses dados; (iv) APEC Privacy Framework, publicado pela Cooperação Econômica da Ásia Pacífico - APEC em 2005. O padrão europeu advém de normas contidas exclusivamente no ii e iii, enquanto o padrão global é o denominador comum a todas elas. Atualmente, já é possível somar na lista o então *General Data Protection Regulation* (Regulamento nº 679/2016 ou GDPR).

A análise das decisões de adequação proferidas pela Comissão Europeia teve como fio condutor a delimitação destes critérios – porém, não ficou limitadas a eles. Conforme será possível notar em diversos casos, estes critérios foram explorados de forma insuficiente nas decisões de adequação estudadas neste trabalho.

Com isto dito, passa-se à apresentação da estrutura desta dissertação. O presente trabalho está dividido em cinco capítulos, incluindo esta Introdução (Capítulo 01) e a Conclusão (Capítulo 05). O Capítulo 02 contextualiza (i) o fenômeno de proliferação de legislações gerais de proteção de dados em diversos países; (ii) distingue a proteção e evolução do direito à privacidade das regras de proteção de dados pessoais; (iii) apresenta o contexto regulatório internacional de tentativas de alinhar interesses para harmonização de regras que não restringissem de forma injustificada o comércio internacional e (iv) contextualiza os fatores tecnológicos que contribuíram para as preocupações de fluxos de dados entre fronteiras e de aplicação de regras distintas de proteção a depender do território do tratamento.

Em seguida, o Capítulo 03 está dividido em dois grandes eixos. O primeiro eixo traz uma análise comparativa entre Diretiva 95/46/CE e GDPR, de forma a compreender quais alterações ocorreram no quadro normativo do regime de transferência internacional de dados pessoais europeu. A própria aprovação do GDPR ficou conhecida como "modernização" de regras de proteção de dados pessoais europeus. Compreender essa chamada evolução aplicada às regras de transferência internacional é importante para os fins desta dissertação, que pretende contribuir para a literatura sobre mapeamento dos denominadores comuns de proteção.

Em seguida, o segundo eixo sistematiza entendimento emitidos sobre o tema pelo *Article 29 – Working Party* (WP29), órgão que foi então substituído pelo atual *European Data Protection Board* (EDPB), mas cujos documentos emitidos ao longo dos anos serviram como suporte para a Comissão Europeia e autoridades nacionais dos países membros da União Europeia, tanto a respeito do tema da transferência internacional quanto em relação a demais temas associados ao tratamento de dados pessoais. Neste capítulo, ainda, é introduzido o caso dos Estados Unidos, visto que a decisão do Tribunal de Justiça da União Europeia (TJUE) invalidando o acordo *Safe Harbor* EUA-UE traz um panorama e histórico importante para entendimento da decisão de adequação vigente, proferida pela Comissão Europeia sobre o regime de proteção de dados dos Estados Unidos (esta tratada em conjunto com as demais decisões no capítulo a seguir – limitada ao que disposto no *Privacy Shield*).

Por fim, o Capítulo 04 apresenta os achados de cada decisão avaliada, sendo cada uma delas expostas em três grupos separados. O primeiro compreende aquelas decisões proferidas entre os anos de 2000 e 2012 ainda sob a Diretiva 95/46/CE (Suíça, Canadá, Guernsey, Argentina, Ilha de Man, Jersey Andorra, Ilha Faroé, Israel, Nova Zelândia, Uruguai). O segundo compreende a decisão a respeito dos Estados Unidos, o qual, conforme se verá, possui relação complexa estabelecida com a União Europeia já desde os anos 2000 (quando da celebração do Acordo *Safe Harbor*) até os dias atuais. Por último, destaca-se a decisão do Japão, sendo a primeira proferida sob o atual GDPR.

2 CONTEXTUALIZANDO O TEMA: A EVOLUÇÃO REGULATÓRIA DO FLUXO DE DADOS ENTRE FRONTEIRAS

2.1 As leis de proteção de dados em contexto

A LGPD prevê um capítulo específico para disciplinar as atividades de transferência internacional de dados pessoais (Capítulo V – Da Transferência Internacional de Dados). Trata-se de Capítulo que disciplina as licenças necessárias para que empresas, organizações ou outras entidades possam transferir dados para além da jurisdição brasileira.

Mais especificamente, a LGPD define transferência internacional de dados em seu artigo 5º, inciso XV, como "transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro" e, em seu artigo 33 e incisos I a IX, a LGPD passa a dispor sobre as hipóteses legais que autorizam a transferência de dados pessoais para fora do país. Conforme se vê, a redação do dispositivo dispõe que a transferência internacional "somente é permitida" quando cumprido com os requisitos expressos pela LGPD em seus incisos.

Este capítulo possui inspiração no texto do GDPR, aprovado pelo Parlamento Europeu e o Conselho da Europa, em 27 de abril de 2016, e na antiga e revogada Diretiva 95/46/CE, igualmente aprovada pelo Parlamento Europeu e Conselho da Europa, em 24 de outubro de 1995. O GDPR também dispõe de um Capítulo V em que versa sobre "Transferências de dados pessoais para países terceiros ou organizações internacionais". Muitas das hipóteses legais que autorizam a transferência para países terceiros contidas no Capítulo V da LGPD possuem relação com aquelas previstas no GDPR ou na Diretiva 95/46/CE, em seu Capítulo IV – Transferência de Dados Pessoais para Países Terceiros, revogada pelo GDPR.

A aprovação da LGPD pelo Brasil o incluiu na lista de países com legislações gerais de proteção de dados pessoais, cuja aplicação é transversal a todos os setores da economia e engloba atividades de tratamento desenvolvidas nos setores público e privado. Conforme aponta a literatura, a LGPD participa de um movimento recente de proliferação de leis de proteção de dados ao redor do mundo. Nesse sentido, Greenleaf (2019) destaca que somente entre o ano de 2017 e 2018 houve um crescimento de 10% de leis de privacidade de dados, partindo de 120 jurisdições para 132[1]. Destas 132 jurisdições, a maioria possui aplicação tanto para o setor público como para o privado e atendem padrões mínimos contidos em acordos internacionais[2].

[1] "In 2017-18, the number of countries that have enacted data privacy laws has risen from 120 to 132, a 10% increase. These 132 jurisdictions have data privacy laws covering both the private sector and public sector in most cases, and which meet at least minimum formal standards based on international agreements. At least 28 other countries have official bills for such laws in various stages of progress, including 9 that have introduced or replaced Bills in 2017-18. Many others, in the wake of the GDPR and "modernization" of Convention 108, are updating or replacing existing laws." (GREENLEAF, 2019, p. 1).

[2] GREENLEAF, 2015.

A Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD) também disponibiliza uma lista de todos os países e as respectivas leis de proteção de dados pessoais e privacidade. Conforme disposto no site, trata-se de um levantamento das legislações que versam sobre proteção de dados e privacidade em todo o mundo[3]. Segundo os dados fornecidos, 107 países adotaram legislação para garantir a proteção de dados e a privacidade, sendo 66 deles considerados países em desenvolvimento ou economias em transição. Os números apontam que o continente americano apresenta 9 países sem leis nesse sentido (representando o valor de 26%), enquanto o continente africano apresenta 12 países (22%) e asiático 19 países (32%), de forma que o continente europeu seria o único continente com cobertura total do tema, em que todas as jurisdições possuem leis para garantir a proteção de dados pessoais e a privacidade.

Estes dados sinalizam a importância que a proteção do direito à privacidade e aos dados pessoais vem ganhando nas diversas jurisdições do globo. Este aumento significativo de leis cujo objetivo é adicionar regras mais protetivas em relação aos direitos relacionados à privacidade e aos dados pessoais dialoga diretamente com os desafios que a transformação em curso impulsionada pelo surgimento da internet trouxe à proteção dos dados pessoais, à privacidade e aos direitos fundamentais como um todo.

É a partir destes impasses que as leis de proteção de dados pessoais visam estabelecer regras, obrigações e responsabilidades aos agentes participantes das atividades de tratamento de dados pessoais de forma a garantir proteção aos titulares dos direitos fundamentais da privacidade e da liberdade, a autodeterminação informativa e o livre desenvolvimento da personalidade, ao mesmo tempo em que garante ao mercado segurança jurídica, o desenvolvimento econômico, tecnológico e a inovação. Estes objetivos são inclusive positivados como fundamento da disciplina de dados pessoais na LGPD (artigo 2º, incisos I a VII)[4], semelhante ao objetivo do GDPR, artigo 1º, (2)[5], o qual ainda possui suporte de seus Considerandos, como exemplo os (2)[6] e (4)[7].

---

[3] Disponível em <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx>. Acesso em: 15.04.2020.

[4] "Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais." (BRASIL, 2018, art. 2).

[5] "Art. 1 (2) O presente regulamento defende os direitos e as liberdades fundamentais das pessoas singulares, nomeadamente o seu direito à proteção dos dados pessoais."(UNIÃO EUROPEIA, 2016, art. 2).

[6] "(2) Os princípios e as regras em matéria de proteção das pessoas singulares relativamente ao tratamento dos seus dados pessoais deverão respeitar, independentemente da nacionalidade ou do local de residência dessas pessoas, os seus direitos e liberdades fundamentais, nomeadamente o direito à proteção dos dados pessoais. O presente regulamento tem como objetivo contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social, a consolidação e a convergência das economias a nível do mercado interno e para o bem-estar das pessoas singulares." (UNIÃO EUROPEIA, 2016, art. 2).

[7] "(4) O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita

O desenvolvimento da internet também impulsionou aumento da capacidade e do fluxo de dados entre fronteiras, trazendo luz aos capítulos das leis que buscam disciplinar as atividades de transferência de dados entre fronteiras. No GDPR, por exemplo, o Considerando (6) evidencia que a "evolução tecnológica e a globalização criaram novos desafios em matéria de proteção de dados pessoais". Por conta desta evolução, o Considerando ainda ressalta que as novas tecnologias permitem a utilização de dados numa escala sem precedentes, seja pelo setor público ou pelo privado, bem como contribuiu para a disponibilização de informações pessoais de forma pública e global. Nesse sentido, as novas tecnologias contribuem, para além da transformação da economia e da vida social, para a facilitação do fluxo de dados entre fronteiras.

Apesar do Considerando do GDPR estar preocupado com o fluxo de dados cuja natureza é pessoal, é interessante ressaltar que o fluxo de dados (seja pessoal ou não) se tornou tão importante que em 2014, por exemplo, foram responsáveis por aumentar o PIB mundial em pelo menos 10%, valor que totalizou U$ 7,8 trilhões (MANYIKA et al., 2016, p. 1). Este fluxo cresceu 45 vezes de 2005 para 2015 e seu número tende a aumentar mais nove vezes até 2020, considerando a expansão e surgimento de novos e-commerce, sites de buscas, vídeos, comunicação e o fluxo de tráfego interno de empresas (MANYIKA et al., 2016, p. 1)[8].

Como se vê, o fluxo de dados pode ser composto por dados de diversa natureza e, dentre eles, estão compreendidos os dados considerados pessoais: objeto de interesse do presente trabalho. Os dados pessoais compõem o comércio internacional ao menos de duas formas distintas. Em uma primeira função, podem ser vistos como acessórios, facilitadores e auxiliares na entrega convencional de produtos e serviços que ocorrem nas transações internacionais. Todavia, em uma segunda função, estes dados também veem ganhando papel importante ao obterem valor econômico de troca intrínseco[9], cotado como o próprio produto da transação comercial. Nas duas hipóteses descritas, os agentes de tratamento que lidem com os dados pessoais têm que respeitar as regras dispostas nas leis sobre proteção de dados pessoais, as quais podem limitar o fluxo dos dados entre fronteiras, as formas de seu tratamento e o seu respectivo local de armazenamento.

Neste contexto, tem-se ressaltado o papel desempenhado pelas plataformas digitais, as

todos os direitos fundamentais e observa as liberdade e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística." (UNIÃO EUROPEIA, 2016, art. 2).

[8] "While flows of goods and finance have lost momentum, used cross-border bandwidth has grown 45 times larger since 2005. It is projected to grow by another nine times in the next five years as digital flows of commerce, information, searches, video, communication, and intracompany traffic continue to surge." (MANYIKA et al., 2016, p. 1).

[9] "In addition to this ancillary role in delivering goods and services, data has intrinsic value when assembled into databases for use in developing artificial intelligence (AI) capabilities or in enabling targeted marketing. Data for this purpose is acquired through what is effectively barter exchange: firms provide the "free" service of use of their platforms in implicit exchange for the data such use generates. This form of exchange leaves no paper trail in the form of receipts or payments and is thus difficult to measure – even in a purely domestic context, let alone on a cross- border basis." (CIURIAK; PTASHKINA, 2018, p. 3).

quais, por exemplo, são apontadas como agentes capazes de mudar substancialmente a forma de se fazer negócio entre fronteiras, sendo grandes vetores responsáveis pela diminuição dos custos de interação e transação internacional (MANYIKA et al., 2016, p. 1)[10]. O seu surgimento também foi capaz de transformar os agentes da transação comercial internacional. Em outras palavras, aponta-se que o cenário do comércio internacional deixa de ser composto somente por grandes multinacionais e passa a poder contar com a participação de pequenas empresas e startups, cujas atividades negociais passam a ter escala global, permitida por conta do fácil acesso à internet. Diante desse cenário, as pequenas empresas e as startups passaram a poder integrar o cenário do comércio internacional com mais facilidade, adotando o papel do que se convencionou chamar de micros multinacionais (MANYIKA et al., 2016, p. 1)[11].

Este cenário é alimentado pelo desenvolvimento de tecnologias que buscam extrair valor de dados pessoais ou, ainda, precisam deles como acessórios para concluir transações comerciais entre fronteiras (entregas convencionais de produtos e serviços). Nessa linha, é ainda possível ressaltar a relevância do surgimento de tecnologias e inteligências de dados que intensificaram e facilitaram os tipos de transferência, compartilhamento e tratamento de dados em geral. Este trabalho introduz, brevemente, estas transformações, com recorte específico dado para (i) o desenvolvimento da *world wide web*, (ii) o surgimento da computação em nuvem e (iii) o modelo de negócio do marketing direto, por meio de implementação de cookies e tecnologias de *adtechs*. No caso de implementação de cookies, destaca-se aqueles cuja finalidade está além da necessidade de coletar informação para garantir funcionalidades de sites, mas abrange, sobretudo, aqueles cookies cuja função é sustentar o modelo de negócio na internet conhecido como mercado de preço zero - em que não há contraprestação monetária pelo usuário em relação ao serviço acessado. Trata-se da monetização dos dados pessoais em troca de serviços.

Por fim, destaca-se que a transformação digital[12], segundo sustentado por Schwab (2016, p. 14), fundador e presidente executivo do Fórum Econômico Mundial, compõe o que ele denomina de quarta revolução industrial. Nessa linha, para que os países possam garantir que essa revolução seja empoderadora e centrada no ser humano, o autor pontua a necessidade de articulação a nível global e de cooperação entre diversos interesses da sociedade:

> Moldar a quarta revolução industrial para garantir que ela seja empoderadora e centrada no ser humano – em vez de divisionista e desumana – não é uma tarefa

[10] "Digital platforms change the economics of doing business across borders, bringing down the cost of international interactions and transactions. They create markets and user communities with global scale, providing businesses with a huge of potential customers and effective ways to reach them." (MANYIKA et al., 2016, p. 1).

[11] "Small businesses worldwide are becoming "micro-multinationals" by using digital platforms such as eBay, Amazon, Facebook, and Alibaba to connect with customers and suppliers in other countries. Even the smallest enterprises can be born global: 86 percent of tech-based startups we surveyed report some type of cross-border activity. The ability of small businesses to reach new markets supports economic growth everywhere." (MANYIKA et al., 2016, p. 8).

[12] Atualmente, para além dos avanços digitais que serão introduzidos nesta dissertação, já está em voga tecnologias que usam análise de big data, inteligência artificial e internet das coisas. Por conta de um limite temporal e qualitativo, optou-se por explorar nesta dissertação as implicações decorrentes da web, computação em nuvem e cookies.

> para um único interessado ou setor, nem para uma única região, ou indústria ou cultura. Pela própria natureza fundamental e global dessa revolução, ela afetará e será influenciada por todos os países, economias, setores e pessoas. É, portanto, crucial que nossa atenção e energia estejam voltadas para a cooperação entre múltiplos stakeholders que envolvam e ultrapassem os limites acadêmicos, sociais, políticos, nacionais e industriais. As interações e colaborações são necessárias para criarmos narrativas positivas, comuns e cheias de esperança que permitam que indivíduos e grupos de todas as partes do mundo participem e se beneficiem das transformações em curso. (SCHWAB, 2016, p. 14)

O autor (SCHWAB, 2016, p. 12) ainda traz três razões que sustentam sua convicção da ocorrência de uma quarta – e distinta – revolução. Sendo elas: (i) velocidade: esta revolução estaria ocorrendo em um ritmo exponencial (e não linear como nas demais), em que novas tecnologias geram outras mais novas e cada vez mais qualificadas; (ii) amplitude e profundidade: tendo a revolução digital como base e combinando várias tecnologias, o que estaria levando para mudanças de paradigma sem precedentes na economia, nos negócios, na sociedade e nos indivíduos; (iii) impacto sistêmico: envolvendo a transformação de sistemas inteiros entre países e dentro deles, bem como em empresas, indústrias e em toda a sociedade.

Diante da amplitude que os debates envolvendo a revolução digital podem tomar, conforme aqui evidenciado, esta dissertação apresenta um recorte focado na relação entre transferência internacional de dados pessoais, internet e regulação.

2.2 A diferença entre proteção de dados pessoais e privacidade

O direito à proteção dos dados pessoais ganhou importância nas últimas décadas como um direito autônomo e independente daquele relacionado ao direito à privacidade. Não se trata de dizer que um não possui relação com o outro e nem mesmo que, muitas das vezes, ambos possam se sobrepor, mas trata-se de reconhecer juridicamente que cada um deles possui escopo de proteção independente e autônomo.

A autonomia desses direitos já vem sendo reconhecida pela própria literatura, bem como já é positivada no direito da União Europeia desde 2000, quando a Carta de Direitos Fundamentais da União Europeia (CDFUE) definiu distintamente a proteção do direito à vida privada em seu artigo 7º[13] e do direito à proteção dos dados pessoais em seu artigo 8º[14]. Enquanto o primeiro dispõe sobre o respeito à vida privada e familiar com enfoque no domicílio e comunicação, o segundo possui escopo mais abrangente cuja proteção se estende à garantia de um tratamento

[13] "Art. 7º - Respeito pela vida privada e familiar: Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações."(UNIÃO EUROPEIA, 2000, Art. 7).

[14] "Art. 8º - Proteção de dados pessoais: 1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legitimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente."(UNIÃO EUROPEIA, 2000, Art. 8).

dos dados pessoais de forma leal, para fins específicos e com o consentimento do titular dos dados pessoais ou com outro fundamento legítimo previamente estipulado em lei.

Nesse mesmo sentido, reconhece Queiroz (2019):

> Assim, muito do que está incluído no âmbito do direito à proteção dos dados pessoais não importa ao direito à privacidade – eis o grande motivo pelo qual não se pode dizer que o direito à proteção de dados pessoais se limita a "um aspecto" do direito à privacidade, como se estivesse inteiramente nele contido.
>
> Ao contrário do direito à privacidade, o direito à proteção dos dados não faz, em princípio, um filtro substantivo sobre a qualidade do dado para decidir se ele está ou não em seu escopo: se é dado pessoal, interessa ao direito da proteção de dados pessoais, ainda que não seja sensível à privacidade do titular. (QUEIROZ, 2019, p. 30)

Em relação à doutrina relacionada aos estudos da privacidade, Doneda (2019, p. 30) ressalta que a doutrina moderna teve início com a publicação do artigo de Warren e Brandeis, intitulado *The right to privacy*, na revista de Harvard, em 1890[15]. Neste artigo, os autores envidam esforços para diferenciar a proteção da privacidade das demais esferas que possuem proteção jurídica[16], como, por exemplo, da sua independência do direito autoral, do direito à propriedade, do direto à compensação por ofensa, difamação ou calúnia. Em relação à delimitação e independência entre privacidade e direito autoral, por exemplo, Warren e Brandeis (1890, p. 201) destacam[17]:

> Um homem registra em uma carta a seu filho, ou em seu diário, que ele não jantou com a sua esposa em um certo dia. Ninguém em cujas mãos esses papéis caiam poderia publicá-los ao mundo, mesmo que a posse dos documentos fosse obtida legitimamente; e a proibição não se restringiria à publicação de uma cópia da própria carta ou da anotação do diário; a restrição se estende também a uma publicação do conteúdo. Qual é o bem que está protegido? Certamente, não o ato intelectual de registrar o fato de o marido não jantar com a esposa, mas o fato em si. Não é o produto intelectual, mas a ocorrência doméstica. (WARREN; BRANDEIS, 1890, p. 201) TRADUÇÃO LIVRE.

Os autores ainda continuam em momento adiante do artigo e afirmam que a proteção do pensamento, sentimentos e emoções expressadas por meio de uma escrita ou pela arte é

[15] Warren e Brandeis (1890).

[16] "O artigo de Warren e Brandeis reflete a tendência a uma fundamentação diversa para a proteção da privacidade, desvinculada do direito de propriedade. Um de seus pontos centrais é a observação de que o princípio a ser observado na proteção da privacidade (no caso específico, na publicação de escritos pessoais) não passa pela propriedade privada, porém pela chamada inviolate personality. Nessa evocação de um direito de natureza pessoal encontramos, com todas as inúmeras ressalvas a serem feitas ao se tratar de um sistema jurídico de fundamentação diversa da civil law, o eixo em torno da proteção da pessoa humana que será determinante na proteção da privacidade no século seguinte." (DONEDA, 2019, p. 124).

[17] "A man records in a letter to his son, or in his diary, the he did not dine with his wife on a certain day. No one into whose hands those papers fall could publish them to the world even if possession of the documents had been obtained rightfully; and the prohibition would not be confined to the publication of a copy of the letter itself, or of the diary entry; the restraint extends also to a publication of the contents. What is the thing which is protected? Surely, not the intellectual act of recording the fact that the husband did not dine with his wife, but the fact itself. It is not the intellectual product, but the domestic occurrence." (WARREN; BRANDEIS, 1890, p. 201).

meramente um exemplo de aplicação do direito de ser deixado só[18]. Sobre este entendimento marcado pelo individualismo da concepção da privacidade, Doneda (2019, p. 31) destaca a importância do artigo, mas ressalta a necessidade de colocá-lo em contexto, sendo necessário a consciência de que a privacidade engloba questões cada vez mais complexas[19].

Sobre isto, o artigo *Privacy as Trust: Sharing Personal Information in a Network World*, de Ari Ezra Waldman, de 2015, busca trazer nova concepção ao direito à privacidade. Conforme aponta, a privacidade é traçada por muitos como sendo uma questão de escolha, autonomia e liberdade individual[20]. Atualmente, o autor argumenta que a privacidade, devido à pré-condição do mundo moderno de compartilhamento de informação, deve ser vista como um direto que protege relações de confiança. Assim, para o autor, a peça que falta nas discussões sobre privacidade diz respeito ao tema da confiança.

Diante disso, a partir da retomada de estudos desenvolvidos no campo da sociologia, o autor esclarece seu entendimento sobre confiança, ressaltando a sua necessidade para se estabelecer contextos de compartilhamento de informação. Vejamos[21]:

> Neste artigo, emprego uma definição geralmente aceita de confiança interpessoal originada da literatura sociológica: confiança é uma expectativa em relação às ações e intenções futuras de determinadas pessoas ou grupos de pessoas. Isto é, para usar uma frase dos sociólogos J. David Lewis e Andrew Weigert, uma "necessidade funcional para a sociedade"porque, entre outras coisas, lubrifica as rodas do compartilhamento efetivo: você interage quando confia. Neste artigo, argumento que as esferas da privacidade refletem as esferas da confiança: quando confiamos, compartilhamos; quando não confiamos, não compartilhamos. Sabemos disso porque nosso senso de quando nossa privacidade é invadida é semelhante ao senso de violação de nossa confiança. (WALDMAN, 2015, p. 564) TRADUÇÃO LIVRE.

[18] "These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the mere general right to be let alone." (WARREN; BRANDEIS, 1890, p. 205).

[19] "Resta, no entanto, um elo de continuidade entre a privacidade como vista pelos seus modernos "fundadores" – Warren e Brandeis – e o complexo problema em que ela se transformou: o centenário diagnóstico realizado pelos autores, à época advogados em Boston, continua valioso, tanto que seu artigo The right to privacy é até hoje lido e citado com invejável constância. Para a sua interpretação, no entanto, deve-se valer da consciência de seus desdobramentos e da constatação de que a privacy hoje compreende algo muito mais complexo do que o isolamento ou a tranquilidade – algo que o próprio Brandeis, tendo se ocupado do assunto posteriormente, tinha ciência." (DONEDA, 2019, p. 31).

[20] Como aponta Bygrave (2010, p. 172), a forma individualista de abordar a privacidade parece ser uma característica que aparece em diversos países (incluindo os Estados Unidos, o qual o autor faz menção em seu artigo). Contudo, o autor também destaca que existe certa variação deste paradigma entre países e culturas, como no caso da Alemanha em comparação com o paradigma americano. O primeiro país possui forte jurisprudência constitucional no sentido de que a proteção dos dados é garantia para condições necessárias de participação do indivíduo na vida pública e para assegurar a democracia. (BYGRAVE, 2010, p. 172).

[21] "In this article, I employ a generally accepted definition of interpersonal trust from the sociological literature: trust is an expectation regarding the future actions and intentions of particular people or groups of people. It is, to use a phrase from the sociologists J. David Lewis and Andrew Weigert, a "functional necessity for society"because, among other things, it greases the wheels of effective sharing: you interact when when you trust. In this article, I argue that spheres of privacy mirror spheres of trust: when we trust, we share; when we do not trust, we do not share. We know this because our sense of when our privacy is invaded is similar to the sense of our trust being breached."(WALDMAN, 2015, p. 564).

Em outra publicação, Waldman (2018, p. 29) continua seu argumento e desenvolve que a confiança é condição necessária para o contexto de compartilhamento na sociedade da informação. Exemplos disso, segundo o autor, é que cada vez mais CPOs (*Chief Privacy Officers*) estão preocupados em ganhar confiança de seus usuários, assim como o desenho das interfaces e a interação com as empresas passaram a incorporar esta palavra, como nos casos em que a Apple pergunta a seu usuário antes de permitir compartilhamento entre plataformas se este "confia neste computador" ou, ainda, Facebook pergunta a seus usuários sobre "afinal, quão confiável é o Facebook em geral?". Como busca relacionar o autor, trata-se de uma relação em que a confiança é o núcleo das nossas expectativas da garantia da privacidade (WALDMAN, 2018, p. 50) e fundamental, portanto, para que se tenha interações baseadas no compartilhamento[22].

Diante desta concepção da privacidade, o que o autor pretende superar é a visão de que a privacidade depende de uma contextualização do que é público (a dicotomia entre o público e privado), derivada da concepção desenvolvida já na época de Warren a Brandeis de ser um direito de ser deixado só. Para o autor, não é surpresa que o direito à privacidade no mundo de hoje reflete as teorias convencionais que relacionam a privacidade ao sigilo, confidencialidade, autonomia e separação do público e privado (o que estariam refletindo pensamentos desenvolvidos por Locke e Kant)[23].

Mais especificamente, nesta concepção tradicional do direito à privacidade, o autor pontua duas perspectivas principais: (i) a negativa, em que a privacidade protege o direito de separação e exclusão em relação à alguma coisa ou alguém (*privacy as freedom from*) e (ii) a positiva, a separação é vista como necessária para atingir algum propósito, como oportunidade de crescer, desenvolver e perceber o potencial humano de forma livre (*privacy as freedom for*)[24].

A forma negativa da privacidade é sustentada a partir da ideia da liberdade individual em face de algo ou alguém. Neste sentido, é negativa porque garante a liberdade de não ocorrer alguma coisa, configurando hipóteses em que se argumenta pela liberdade de não ser invadido,

[22] "Trust pervades the privacy landscape. When chief privacy officers (CPOs) talk about privacy, they talk about it in terms of gaining user trust. "[T]he end objective," one CPO reported, "is always: what's the right thing to do to maintain the company's trusted relationship with our employees, with our clients, with any constituency in society that has a relationship to us." In a recent article in the Harvard Business Review, furthermore, several technology company executives argued that the way to ensure that increasingly privacy savvy users will continue to share data is to gain user trust and confidence. Apple knows this already. When trying to log on to iCloud on a new device or desktop, Apple asks us if we "Trust this browser?" and requires us to enter a 6-digit code before we can gain access. And iPhones using iOS 8 or higher also ask if we "Trust this computer?" before sharing any data across platforms. Facebook also understands that we think about our privacy in terms of trust. For example, in 2013, Facebook asked its users, "How trustworthy is Facebook overall?" A spokesperson explained that Facebook was just looking for feedback to improve service and enhance user experiences. But there is likely much more to it. We know that Facebook is an inherently social tool designed to create, foster, and expand social interaction. We also know that Facebook routinely tinkers with its user interface to inspire user trust and, in turn, sharing. Its committee of Trust Engineers, for example, plays with wording, multiple choice options, the order of questions, designs, and other tools to encourage users to honestly report what they do not like about posts they want taken down. That may be an important goal, but it shows that Facebook is well aware that trust and sharing are linked." (WALDMAN, 2018, p. 49).

[23] Waldman (2015, p. 566).

[24] Waldman (2015, p. 567-585).

a liberdade de não ser violado pelo Estado ou por qualquer ator privado. A forma positiva da privacidade é sustentada a partir da liberdade individual para alcançar algo. Neste sentido, a privacidade é necessária como condição para conquista da independência e autonomia do indivíduo. É positiva porque garante a liberdade para se alcançar outro objetivo, como a autonomia, a formação de ideias e a concepção da personalidade. Estas duas formas de enxergar a privacidade partem da teoria liberal e garantem a proteção dos indivíduos contra o governo, a proteção das suas informações e dos respectivos espaços privados[25].

Já sobre o que consiste a evolução da carga jurídica vinculada à proteção dos dados pessoais, esta dissertação contribui, em certa medida, para estudos que pretendem descrever o seu desenvolvimento, trazendo questões relevantes que impuseram desafios à sua proteção, incluindo a evolução de instrumentos regulatórios que pretendiam estabelecer mecanismos concretos de proteção deste direito, os limites funcionais das organizações internacionais a respeito da garantia desta proteção e a saída encontrada pela União Europeia para garantir os seus padrões de proteção às demais jurisdições do globo. Com isto em vista, este estudo centraliza as avaliações realizadas pela Comissão Europeia a respeito do sistema jurídico de proteção dos dados pessoais de países terceiros. Estes pontos são aprofundados nos tópicos a seguir.

2.3 A evolução dos modelos regulatórios do fluxo de dados pessoais entre fronteiras

2.3.1 Medidas de restrição do fluxo de dados entre fronteiras

Conforme aponta Ferracane (2017), restrições ao fluxo dos dados não são novidades, mas tiveram um crescimento rápido na última década. Ainda, a autora exemplifica que em regimes mais rígidos de privacidade existem regras de uso local de *data centers* e de proibição total da transferência para outros países. A autora aponta para uma via de mão dupla: os dados são a causa e a própria vítima dessas medidas. Assim, nas palavras da autora[26]:

> A revolução dos dados é tanto a razão por trás dessa tendência e a vítima não almejada destas políticas. A crescente dependência de dados em nossas econo-

[25] Formas de repensar a visão tradicional liberal do direito à privacidade vem sendo desenvolvida para garantia de um instrumental teórico que possa lidar com os novos desafios trazidos pela internet. Estes autores acreditam que a concepção tradicional da privacidade seria muito rígida e inadequada para resolver os problemas modernos, portanto, sugerem uma concepção da privacidade baseada na confiança entre atores privados, indivíduos e intermediários da internet e entre pessoas interagindo online e offline. Nesta linha, o direito à privacidade seria mais efetivo se focado em proteger as relações de confiança, construída a partir de bases sociológicas. Para mais aprofundamento no tema, ver: Waldman (2015).

[26] "The data revolution is both the reason behind this trend and the unwanted victim of these policies. The increasing reliance on data in our economies has raised concerns among policymakers that felt the need to respond promptly to this development with new legislation. However, the novelty of the data revolution and the difficulty of policymakers to grasp its transformational impact on the economy led to responses that impose significant costs on the economy (ECIPE, 2014; ECIPE, 2016) and on foreign businesses (USITC, 2014)." (FERRACANE, 2017, p. 2).

> mias levantou preocupações entre os formuladores de políticas que sentiram a necessidade de responder prontamente a esse desenvolvimento com nova legislação. No entanto, a novidade da revolução dos dados e a dificuldade dos formuladores de políticas de captar seu impacto transformacional na economia levaram a respostas que impõem custos significativos à economia (ECIPE, 2014; ECIPE, 2016) e às empresas estrangeiras (USITC, 2014). (FERRACANE, 2017, p. 2) TRADUÇÃO LIVRE

Mais especificamente, a autora esclarece sobre o entendimento do que seria as restrições ao fluxo de dados. Em relação à perspectiva do comércio, restrições ao fluxo de dados podem ser definidas como todas aquelas medidas que aumentam o custo de condução do negócio entre fronteiras, seja por meio da imposição de que empresas devem manter os dados dentro de uma fronteira determinada, seja por meio de requisitos específicos para autorização da transferência para fora de um país (FERRACANE, 2017, p. 2). Apesar de diversos modelos regulatórios serem possíveis dentro desse espectro, Ferracane (2017, p. 3) aponta que todos eles compartilham uma mesma característica: entidades privadas são forçadas a manter os dados localmente ou têm que arcar com altos custos para o envio ou tratamento dos dados fora do país.

Dentre as formas possíveis de se limitar o fluxo de dados entre fronteiras, Ferracane (2017, p. 3) explica dois grandes modelos[27]. O primeiro em que se tem medidas que variam em relação ao tipo de restrição imposta ao tratamento do dado, como (i.a) requisitos de armazenamento local de dados; (i.b) requisitos de armazenamento e processamento local de dados pessoais e (i.c) proibição de transferência de dados, casos em que se requer o armazenamento local, processamento local e acesso local. O segundo em que se tem restrições condicionais ao fluxo de dados, sendo elas (i) aplicadas ao país terceiro receptor dos dados ou (ii) aplicadas aos agentes de tratamento, como nos casos em que as condições recaem sobre o controlador e operador dos dados pessoais em tratamento.

Estas medidas são vistas como restrições ao fluxo de dados entre fronteiras porque impõem barreiras ou dificultam o desenvolvimento desta atividade, o que, conforme argumentado por certos autores[28], colocam empresas estrangeiras em desvantagem, constituindo medidas

[27] A classificação trazida por Ferracane é uma dentre outras existentes na literatura sobre o tema. A escolha por esta autora se deu por conta da funcionalidade de sua classificação. Conforme se verá ao longo desta dissertação, de fato, trata-se de uma classificação próxima ao contexto de leis e outras normas que restringiram o fluxo de dados pessoais. Como o escopo deste trabalho não é aprofundar na literatura sobre o tema de classificação dos tipos de restrição do fluxo de dados entre fronteiras, optou-se por explorar o conteúdo trazido por Ferracane dada a sua importância e contribuição funcional. Todavia, para mais informações sobre o tema, consultar: Aaronson (2015), Cory (2017), Ciuriak e Ptashkina (2018).

[28] "Despite the significant benefits to companies, consumers, and national economies that arise from the ability of organizations to easily share data across borders, dozens of countries—across every stage of development—have erected barriers to cross-border data flows, such as data-residency requirements that confine data within a country's borders, a concept known as "data localization." Data localization can be explicitly required by law or is the de facto result of a culmination of other restrictive policies that make it unfeasible to transfer data, such as requiring companies to store a copy of the data locally, requiring companies to process data locally, and mandating individual or government consent for data transfers. These policies represent a new barrier to global digital trade. Cutting off data flows or making such flows harder or more expensive puts foreign firms at a disadvantage. This is especially the case for small and solely Internet-based firms and platforms that do not have the resources to deal with burdensome restrictions in every country in which they may have customers. In

protecionistas uma vez que podem manter competidores estrangeiros fora do mercado doméstico (CORY, 2017). Assim, conforme classificação acima, estas atividades podem ir desde regras estritas de localização dos dados em território nacional até medidas impostas por lei que resultam, de fato, em medidas que tornam a transferência internacional de dados inviável ou colocam certos obstáculos para sua conclusão[29].

Quanto ao primeiro tipo de restrição trazida por Ferracane - requisitos de armazenamento local dos dados (i.a) -, trata-se de exigência de que os dados não podem ser transferidos entre fronteiras a não ser que uma cópia seja armazenada nas localidades da jurisdição estatal. Assim, contanto que os dados sejam armazenados ou estejam copiados dentro do país, então eles podem ser tratados no exterior, aqui incluída a possibilidade de serem também armazenados. Trata-se, assim, de exigência de cópia dos dados em território nacional. A autora (FERRACANE, 2017, p. 4) cita como exemplo o caso da Suécia, em que a Lei de Contabilidade (do inglês *Bookkeeping Act*) impõe que documentos como relatórios anuais financeiros e balanços de empresas estejam fisicamente armazenados na Suécia por um período de sete anos.

Quanto ao segundo tipo de requisitos de armazenamento e tratamento local de dados pessoais (i.b), as obrigações recaem na exigência de que as empresas devem tratar os dados em *data centers* localizados no país. Em outras palavras, a empresa só pode tratar dados quando estes estejam armazenados nas localidades da jurisdição. Neste cenário, após o tratamento dos dados, a princípio, não há nenhuma limitação para que estes sejam transferidos para fora. A autora traz o exemplo da Rússia, em que, a partir da emenda na lei de proteção de dados russa, passou a requerer em seu artigo 18 § 5º que os operadores dos dados garantam que o registro, sistematização, acumulação, armazenamento, atualização/alteração e recuperação de dados pessoais dos cidadãos da Federação Russa sejam feitos usando centro de dados localizados em sua jurisdição (FERRACANE, 2017, p. 4).

Sobre o artigo 18, § 5º, Selby (2017, p. 222) explica que a lei não proibi expressamente a cópia de dados pessoais para fora do território russo, trata-se, na verdade, de obrigação de uso de *data center* local enquanto as atividades previamente estipuladas em lei estejam sendo realizadas pelos agentes de tratamento. Ainda, o autor esclarece que a Autoridade de Proteção de Dados Russa, em novembro de 2014, deu orientações quanto à interpretação do artigo no sentido de que é permitida a transferência para fora do território russo aos países signatários da Convenção 108 da Europa desde que obtido o consentimento prévio do titular de dados. Em agosto de 2015, por sua vez, o Ministro de Telecomunicações da Rússia emitiu um "guia não oficial" esclarecendo que as regras de localização de dados não se aplicariam retroativamente, não sendo necessário que dados que já tenham sido transferidos sejam "repatriados". Todavia, conforme aponta Selby

essence, these tactics constitute "data protectionism" because they keep foreign competitors out of domestic markets." (CORY, 2017, p. 2).

[29] "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)." (SELBY, 2017, p. 215).

(2017, p. 223), caso a empresa atualize ou modifique o dado armazenado fora do país, então esta operação deve ocorrer também em servidores localizados no território russo[30].

Quanto ao terceiro tipo apontado por Ferracane de proibição da transferência de dados (i.c), esta recai na obrigação de que os dados devem ser armazenados, tratados e acessados no território da jurisdição. Neste caso, trata-se de proibição expressa aplicada às empresas, que ficam proibidas de enviar os dados para fora. Conforme a autora ainda aponta, a diferença entre este tipo de proibição de transferência dos dados e o tipo explicado anteriormente sobre requisitos de tratamento local de dados diz respeito à proibição de até mesmo fazer cópia dos dados fora da jurisdição, o que poderia ser prejudicial para empresas que possuem subsidiárias em outro país ou até mesmo para garantir a segurança do armazenamento dos dados. Apesar de não haver exemplos de países que apliquem esta medida de forma ampla, a autora cita exemplos de setores específicos e de natureza de dados específicas aplicadas pela Austrália e pelo Canada, vejamos[31]:

> No entanto, algumas jurisdições impõem proibições à transferência de conjuntos de dados específicos. Por exemplo, a Austrália exige que nenhuma informação eletrônica pessoal de saúde seja mantida ou processada fora das fronteiras nacionais. Outro exemplo são duas províncias do Canadá (Colúmbia Britânica e Nova Escócia) que promulgaram leis que exigem informações pessoais mantidas por instituições públicas (como escolas, universidades, hospitais ou outros serviços e agências de propriedade do governo) devem permanecer no Canadá – com apenas algumas exceções limitadas. (FERRACANE, 2017, p. 4) TRADUÇÃO LIVRE

Como se vê, os três níveis deste primeiro modelo apresentam graus de restrição gradativo. Enquanto o primeiro exige o armazenamento de cópia dos dados na jurisdição, o segundo requer que ao longo do tratamento dos dados, empresas utilizem *data centers* locais e, no último modelo, que utilizem *data center* locais com exclusividade, vendando-se qualquer armazenamento em outra jurisdição.

[30] "While the law does not explicitly prohibit operators from transferring a copy of personal data about Russian citizens outside of Russia for processing abroad, the Russian President's staff circulated a non-binding commentary recommending that such data processing should occur only within Russia and off-shore data copying should not be permitted. However, as this is a non-binding commentary, it is unclear whether Russian courts would adopt the same restrictive interpretation proposed by the Executive. Contradicting the Russian President's staff, the Russian data protection authority's (Roskomnadzor) November 2014 interpretation of the law permitted offshore transfers to countries party to the Council of Europe Convention on Data Protection where prior written consent from the data subject had been received. In August 2015, the Russian Ministry of Telecommunications' unofficial guidance agreed with the interpretation of the Russian Data Protection Authority regarding offshore transfers, clarified that the data localization law would not apply retroactively (ie there was no requirement to repatriate Russian citizen's personal data if it had already been transferred abroad for processing) but added that it regarded an entity outside of Russia operating a website 'aimed at the territory of Russia' would be required to comply with the Russian data localization requirements. If an entity updated or modifies existing data stored offshore, then it would be required to be localized onto servers located within Russian territory." (SELBY, 2017, p. 223).

[31] "However, some jurisdictions impose bans on the transfer of specific sets of data. For example, Australia requires that no personal electronic health information is held or processed outside national borders.8 Another example is two provinces of Canada (British Columbia and Nova Scotia) which have enacted laws that require personal information held by public institutions (such as schools, universities, hospitals or other government-owned utilities and agencies) to stay in Canada - with only a few limited exceptions."(FERRACANE, 2017, p. 4).

No que se refere ao segundo modelo, a exigência de condicionar a transferência entre fronteiras estabelece obrigação de que as empresas cumpram com determinados requisitos dispostos em lei para que possam transferir os dados para fora. Dessa forma, a transferência é proibida a não ser que a empresa cumpra com as condições previamente dispostas em leis. Estas condições dizem respeito às exigências aplicadas (ii.a) ao país que receberá os dados; (ii.b) ou às empresas; (ii.c) ou aos dois ao mesmo tempo. Um exemplo dado pela autora dentro desta classificação é o regime europeu de transferência internacional de dados pessoais. Sobre isso, vejamos[32]:

> O regime europeu de proteção de dados é um exemplo típico de regime condicional. De acordo com a legislação europeia, as condições se aplicam ao país destinatário e à entidade responsável pela transferência. No primeiro caso, a empresa pode transferir dados para o exterior para países com um "nível adequado de proteção". No segundo caso, mesmo quando o país destinatário não é considerado adequado, os dados podem ser transferidos e tratados no exterior se o receptor cumprir determinadas condições. (FERRACANE, 2017, p. 5) TRADUÇÃO LIVRE

A partir dos exemplos dados acima, é possível destacar que o tema da regulação dos dados entre fronteiras possui contornos que superam interesses de uma determinada regulação doméstica. A preocupação em relação à forma como os dados são tratados fora do país importa para os temas de transferência internacional de dados, principalmente quando se quer garantir certo controle em relação ao dado e mapeamento quanto ao seu fluxo.

Nesse sentido, Selby (2017, p. 227) esclarece quatro razões que são tipicamente usadas para fundamentar adoção de regras de localização dos dados, sendo estas relacionadas à (i) segurança contra agências de inteligência estrangeira; (ii) promoção da indústria local, uma vez que incentiva o uso de *data centers* localizados no país[33]; (iii) proteção da privacidade e segurança dos titulares de dados e (iv) garantia de cumprimento de obrigações locais e de ordens de agentes responsáveis pelo *enforcement* de regras nacionais (caso de pedido de acesso a dados, por exemplo)[34].

[32] "The European regime of data protection is typical example of a conditional regime. Under European law, conditions apply to both the recipient country and the transferring entity. In the first case, the company can transfer data abroad to countries with an “adequate level of protection”. In the second case, even when the recipient country is not deemed adequate, data can be transferred and processed overseas if the transferee fulfils certain conditions."(FERRACANE, 2017, p. 5).

[33] “The challenge with relying upon the infant industry argument for data localization is that data centres do not really employ any significant numbers of staff. 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.” (SELBY, 2017, p. 229).

[34] “Even if they are willing to provide assistance, the foreign cloud provider may still unintentionally impede the investigation by recording and storing logs in non-standard formats, not logging or retaining records of certain data fields that could be particularly useful for the purposes of the investigation, or by simply failing to provide the needed data in a timely manner. On the other hand, local law enforcement can more easily negotiate or set protocols with the management of a local data centre so as to gain access to the needed information in a timely manner.” (SELBY, 2017, p. 230).

Este tema, no que toca à intersecção com o direito à privacidade e dados pessoais, veio sendo objeto de discussão entre os países em diversos *locus*, dando origem, inicialmente, a instrumentos como (i) as Diretrizes para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais (Diretrizes de 1980), adotada como Recomendação pelo Conselho da OCDE, em 23 de setembro de 1980, e (ii) a Convenção para a Proteção das Pessoas em relação ao Tratamento Automatizado de Dados Pessoais (Convenção 108), do Conselho da Europa, adotada em 28 de janeiro de 1981, sendo o primeiro tratado internacional vinculante sobre proteção de dados pessoais, aberto para assinatura aos demais países. O tópico a seguir descreve a evolução dos dois instrumentos de forma mais detalhada.

2.3.2 A regulação em torno do fluxo de dados entre fronteiras

Conforme apontado no relatório da OCDE (OECD, 2011, p. 7), que explica a evolução da privacidade no contexto de aprovação das Diretrizes de 1980 e descreve os desafios enfrentados nos seus 30 anos posteriores, o debate em torno do tema relacionando privacidade e fluxo de dados pessoais teve como marco inicial o final da década de 1960, com a introdução da primeira geração de computadores[35]. Os anos 70s, por sua vez, foi marcado por diversas iniciativas dentro da OCDE que conduziram as discussões sobre o tema para a elaboração do texto final das Diretrizes de 1980.

Assim, por meio de realização de seminários e criação de grupos de trabalho sobre diversos tópicos que tangenciam a privacidade e o fluxo transfronteiriço de dados, em 1976 o Secretário da OCDE (OECD, 2011, p. 9) destacou que com as inovações trazidas pela tecnologia da informação - principalmente por meio de computadores e do desenvolvimento da telecomunicação -, estabelecia-se novas dimensões aos já antigos métodos tradicionais de manutenção de registros. Estes novos métodos, segundo o Secretário, à medida que se expandem e são automatizados, teriam a capacidade de colocar ainda maiores desafios à privacidade dos indivíduos. Com isto em jogo, o Secretário chama atenção para a necessidade de se criar leis, regulamentos e códigos cuja função é garantir o desenvolvimento equilibrado da tecnologia (OECD, 2011, p. 9).

Em 1977, por sua vez, ocorreu encontro com mais de 300 pessoas dos países membros da OCDE, do setor privado e de organizações intergovernamentais, para discutir sobre o tema do fluxo de dados pessoais e a proteção da privacidade (OECD, 2011, p. 9). Na ocasião, o discurso do Presidente da *Comission Nationale de línformatique et des Libertés* francesa, Louis Joinet, ficou conhecido por destacar o valor econômico e o interesse nacional no fluxo transfronteiriço de dados. Com isto em consideração, o Presidente destacava que a habilidade de armazenar

[35] "Privacy became an issue in the late 1960s because of the convergence of two trends: the postindustrial information revolution and the growing government use of personal data. The advantages of using computers to more efficiently process data were increasingly apparent yet at the same time so too were growing concerns about the possible loss of dignity or the erosion of rights that could result from the misuse of personal data. There was recognition too of the growing awareness in certain circles of the need to empower citizens in claiming their rights." (OECD, 2011, p. 7).

e tratar certos tipos de dados poderia causar distorções entre países, colocando um país em vantagem política e tecnológica sobre o outro (OECD, 2011, p. 10).

Com estas questões e demais outras anunciadas ao longo dos encontros oficiais, criou-se um Grupo de Experts no tema para trabalhar na criação das Diretrizes de forma a estabelecer denominador comum de proteção aos dados pessoais e evitar que países implementassem medidas protecionistas limitando o fluxo de dados entre fronteiras tendo como fundamento a proteção dos dados pessoais e da privacidade. Assim, em 1980 é aprovada a então conhecida Diretrizes de 1980[36], cujo texto original passou por revisão em 2013.

Com isto dito, convém destacar que já na primeira versão das Diretrizes de 1980 se reconhecia impasses importantes para o contorno dos debates que seguem nos próximos anos relacionados à regulação dos dados pessoais entre fronteiras, como: (i) a existência de interesse em comum em conciliar valores como privacidade e liberdades individuais e o livre fluxo de informações; (ii) o fato de que o avanço do tratamento automatizado e dos fluxos transfronteiriços de dados pessoais criam novas formas de relacionamento entre os países e demandam o desenvolvimento de regras e práticas compatíveis; (iii) os fluxos transfronteiriços de dados pessoais são fatores importantes para o desenvolvimento econômico e social; (iv) a legislação doméstica relativa à proteção da privacidade e dos dados pessoais podem dificultar ou impor barreiras injustificadas aos fluxos entre fronteiras.

Este assunto também foi enfrentado pelos Estados Membros do Conselho da Europa, os quais assinaram, em 1981, a Convenção 108. Trata-se do primeiro instrumento internacional vinculativo no tema e cuja participação é aberta para assinatura de países não membros, conforme expressamente estabelece seu artigo 23[37]. Nesse sentido, a Convenção 108 conta com a adesão

[36] Apesar de os princípios da OCDE estarem hoje presentes nas mais variadas legislações de proteção de dados ao redor do mundo e em outros instrumentos internacionais (como a Convenção 108 e na APEC Privacy Framework), à época, o consenso quanto a este núcleo duro de princípios não foi fácil de se alcançar. Vejamos o que descreve o relatório da OCDE: "The hope was that by reaching agreement on a broad set of fundamental principles to protect personal data that could be adopted by the member countries and other nations, there would be less pressure to regulate or attempt to control international data flows. The emphasis on trying to ensure that the measures being introduced to protect personal data would not result in restrictions on transborder data flows runs through the Guidelines. Although there was a broad consensus about the principles and the need to take action, reaching agreement was not easy. According to Justice Kirby, "it is something of a miracle that the OECD Guidelines emerged at all." One of the key challenges facing the Expert Group is described in the Explanatory Memorandum: ...there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth. The Explanatory Memorandum also suggests that there was debate around how the Guidelines should address other "key issues" such as sensitive data, automated data processing, the application to legal persons (corporations, associations), oversight and sanctions, retention periods and other implementation matters, applicable law and exceptions." (OECD, 2011, p. 10).

[37] "Art. 23 – Accession by non-member States 1After the entry into force of this Convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this Convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee. 2 In respect of any acceding State, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe." (COUNCIL OF EUROPE, 1981, Art. 23).

dos 47 Estados Membros do Conselho da Europa, bem como com mais nove integrantes: Argentina (2019), Marrocos (2019), México (2018), Cabo Verde (2018), Tunísia (2017), Senegal (2016), Maurícias (2016), Uruguai (2013)[38].

À similaridade das Diretrizes da OCDE, a Convenção 108 reconhece o dilema envolvendo a regulação do fluxo de dados entre fronteiras. Assim, ao mesmo tempo em que, de um lado, enfatiza em seu Preâmbulo compromissos com a proteção de direitos e liberdades individuais - como o da privacidade -, do outro, ressalta a importância da liberdade de informação independentemente de fronteiras[39]. Sobre isto, reconhece a necessidade de reconciliar estes valores fundamentais, porém competitivos, como o respeito à privacidade e o livre fluxo de informação entre os povos[40].

Para cumprir com os objetivos deste trabalho, destaca-se a seguir breves considerações a respeito de alguns conceitos estipulados nas Diretrizes da OCDE e da Convenção 108 relacionados a (i) dados pessoais; (ii) controlador de dados pessoais e (iii) fluxo transfronteiriço de dados pessoais.

Tabela 1 – Conceitos importantes nas Diretrizes de 1980

Conceitos	**Diretrizes de 1980**
Dados Pessoais	Qualquer informação relacionada a uma pessoa identificada ou identificável.
Controlador de dados pessoais	Parte que, de acordo com a legislação doméstica, é competente para decidir sobre o conteúdo e uso dos dados pessoais, independentemente se tais dados foram coletados, armazenados, tratados ou divulgados por essa parte ou por um agente em seu nome.
Fluxo transfronteiriço	Movimento de dados pessoais através das fronteiras nacionais.

Duas observações são relevantes aqui. A primeira relacionada à extensão do conceito de dados pessoais. A segunda, por sua vez, relacionada às possíveis exceções ao livre fluxo de dados pessoais que poderiam ser estabelecidas entre os países membros da OCDE que adotassem as recomendações das Diretrizes. Adicionalmente, ressalta-se a ausência de utilidade funcional do conceito estabelecido nas Diretrizes a respeito do fluxo transfronteiriço de dados e as mudanças ocorridas após a versão revisada das Diretrizes em 2013.

No que se refere ao conceito de dados pessoais, nota-se, já desde 1980, a adoção de

[38] Mais informações em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=sREdBB35>. Acesso em: 17.04.2020

[39] "Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular, the right to the respect for privacy, taking into account of the increasing flow across frontiers of personal data undergoing automatic processing." (COUNCIL OF EUROPE, 1981).

[40] "Reaffirming at the same time their commitment to freedom of information regardless of frontiers; Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples"(COUNCIL OF EUROPE, 1981).

conceito expansionista de dados pessoais (BIONI, 2016, p. 17)[41], o qual busca retratar um vocabulário cuja intenção é expandir a noção de dado pessoal para além de situações em que uma pessoa é identificada diretamente. Nesse sentido, inclui-se também aqueles dados em que a potencialidade – ainda que remota – é capaz de identificar um indivíduo. Neste último caso, trata-se de uma pessoa identificável, sendo o fator contextual um suporte imprescindível para se aferir o grau de *identificabilidade* de um dado (BIONI, 2016, p. 18)[42].

Já em relação às exceções ao livre fluxo de dados, o seu tratamento se deu originalmente por meio de uma regra e três possíveis exceções. Como regra, as Diretrizes de 1980 dispõem que os países membros devem tomar todas as medidas razoáveis e apropriadas para assegurar que os fluxos transfronteiriços de dados pessoais, incluindo o trânsito através de um país-membro, sejam ininterruptos e seguros. Como exceções, estabelece que os países membros podem restringir os fluxos transfronteiriços de dados pessoais entre si quando (i) algum país membro ainda não tiver observado substancialmente as Diretrizes; (ii) quando a reexportação de tais dados contornar sua legislação doméstica de privacidade ou (ii) em relação a certas categorias de dados pessoais para os quais sua legislação de privacidade interna inclui regulamentações específicas, tendo em vista a natureza desses dados e para os quais o outro país membro não oferece proteção equivalente[43].

Como se vê, a regra das Diretrizes de 1980 sustentava o livre fluxo de dados pessoais, sendo possível abrir exceção à nível nacional fundamentado em três hipóteses específicas. Apesar de ter o livre fluxo como regra, é possível argumentar que as Diretrizes ainda possibilitavam margem considerável de espaço aos países para a restrição do fluxo de dados, desde que devidamente fundamentada em alguma das três exceções descritas acima.

A partir de 2013, o tema passou a ser regulado com certas alterações ao texto original. Em primeiro lugar, as Diretrizes passaram a prever que um controlador permanecerá responsável pelos dados pessoais em seu controle independente da localização geográfica dos dados. Em seguida, estabelece que os países devem se abster de limitar o fluxo de dados entre fronteiras quando o outro país (i) observa as Diretrizes ou (ii) exista salvaguardas suficientes, incluindo mecanismos de *enforcement* das regras e medidas apropriadas estabelecidas pelos controladores, capazes de garantir nível adequado de proteção consistente com aquele estabelecido nas Diretrizes. Por fim, o novo texto esclarece que qualquer limite ao fluxo de dados deve ser proporcional ao risco apresentado e levar em consideração a sensibilidade dos dados, a finalidade e o contexto

41 "O conceito de dado pessoal é um elemento chave pois filtra o que deve estar dentro ou fora do escopo de uma lei de proteção de dados pessoais, demarcando o terreno a ser por ela ocupado. Diferenças sutis em torno da sua definição implicam em consequências drásticas para o alcance dessa proteção. Por isso, compreender se um dado poder ser adjetivado como pessoal é, antes de tudo, um exercício de interpretação detido sobre cada palavra utilizada para prescrever a sua conceituação." (BIONI, 2016, p. 17).

42 "Ainda que divergentes, tais teorizações detêm o mesmo centro gravitacional. Ambas demandam uma análise contextual donde está inserido um dado, aferindo-se o seu grau de identificabilidade para, então, desencadear a compreensão se uma determinada informação está relacionada a uma pessoa identificada ou identificável." (BIONI, 2016, p. 18).

43 "There are, however, exceptions to the presumption of free flow if the other member country does not substantially observe the Guidelines or if the re-export of data would circumvent domestic legislation. Restrictions may also be imposed if there is no equivalent protection for sensitive information." (OECD, 2011, p. 22).

do tratamento.

Uma expressão importante passa a compor a redação do fluxo de dados entre fronteiras das Diretrizes: a garantia de nível adequado de proteção. Contudo, a garantia do nível de proteção, diferente do instituto da decisão de adequação criada pela Diretiva 95/46/CE da União Europeia, não está baseada em uma avaliação geográfica. Tanto é assim que o controlador permanece responsável independentemente da localização dos dados e independentemente da implementação dos mecanismos, desde que os dados estejam em seu controle (OCDE, 2013, p. 30).

No que se refere ao conceito de fluxo de dados transfronteiriços, é possível observar que a definição das Diretrizes pouco adiciona elementos funcionais que busquem contribuir para o que, de fato, significa transferir dados entre fronteiras no mundo digital. Atualmente, este assunto é ainda mais complexo a partir do desenvolvimento tecnológico ocorrido ao longo dos últimos anos. Em outras palavras, as Diretrizes de 1980 trata de forma insuficiente o que significa regular fluxo de dados entre fronteiras. Pode-se argumentar que esta definição mais vaga possui influência tanto devido ao contexto tecnológico da época, quanto a dificuldades de se ter Diretrizes mais precisas devido a divergências para encontrar o seu denominador comum – considerando ainda que o conceito não sofreu alterações com a revisão do texto em 2013[44].

Por sua vez, a Convenção 108 se aplica em contexto de tratamento automatizado de dados pessoais e (i) adotou mesmo conceito de dados pessoais, porém (ii) difere no conceito de controlador e (iii) é silente quanto à definição de fluxo transfronteiriço de dados. A seguir, a tabela resume os três pontos.

Tabela 2 – Conceitos importantes na Convenção 108

Conceitos	**Convenção 108**
Dados Pessoais	Qualquer informação relacionada a uma pessoa identificada ou identificável.
Controlador de dados pessoais	Pessoa física ou jurídica, autoridade pública, agência ou outro órgão competente de acordo com a lei nacional para decidir (a) qual deve ser a finalidade do arquivo automatizado de dados; (b) quais categorias de dados pessoais devem ser armazenadas e (c) quais operações devem ser aplicadas.
Fluxo transfronteiriço	Não há definição.

Em relação ao *fluxo transfronteiriço de dados pessoais*, apesar da ausência de uma definição expressa, o tema é regulado no "Capítulo III – Princípios básicos de aplicação internacional:

[44] De fato, há limites para o conceito estipulado à época de fluxo transfronteiriço de dados pessoais visto o contexto tecnológico que a aprovação das Diretrizes estava inserida. Contudo, a crítica quanto a sua ausência de elementos funcionais continua sendo válida, uma vez que seu conceito nada mais faz do que uma mera descrição superficial do ato de transferir um dado que ultrapassa a fronteira nacional.

fluxo livre e restrições legítimas". Este capítulo estabelece que uma Parte não poderá, com o único propósito de proteção da privacidade, proibir ou sujeitar à autorização especial os fluxos transfronteiriços de dados pessoais destinados ao território da outra Parte. Não obstante, pode haver restrições ao fluxo entre fronteiras de dados pessoais nos casos em que há um risco sério e real de quando (i) não há proteção equivalente da outra Parte signatária e (ii) a fim de evitar que a transferência resulte em violação da Convenção nos casos em que a transferência é feita a partir de seu território para o território de um Estado não signatário através de um intermediário signatário da Convenção.

O Protocolo Adicional à Convenção para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais, de 2001, do Conselho da Europa, altera a Convenção 108[45]. O Protocolo traz duas inovações principais (i) requisitos específicos quanto à criação de autoridades supervisoras nacionais responsáveis, sobretudo, pelo cumprimento das leis e regulamentos adotados pelos países para dar cumprimento à Convenção 108 e (ii) requisitos específicos para que as transferências a serem realizadas a países terceiros não signatários da Convenção 108 passem a ser realizadas mediante garantias de oferecimento de nível adequado de proteção. Estas garantias, segundo manifestação oficial do próprio Conselho da Europa, podem ser implementadas mediante cláusulas contratuais específicas e normas corporativas globais[46].

Conforme é possível notar, a Convenção 108 foi alterada em 2001 e passou a prever a necessidade de se garantir o nível adequado de proteção para transferências a países não signatários. Esta previsão antecede a alteração das Diretrizes da OCDE, a qual passou a contar com termo similar somente em sua versão atualizada em 2013.

No entanto, apesar da previsão de implementação de garantias necessárias para assegurar o nível de proteção adequado da transferência ao destinatário localizado em um país terceiro, a Convenção também passa a dispor de outras três hipóteses de autorização, como nos casos em que (i) tenha-se obtido consentimento explícito, específico e livre, após informado dos riscos

[45] "Building on Article 1 of the additional protocol, the modernised Convention complements the catalogue of the authorities' powers with a provision that, in addition to their powers to intervene, investigate, engage in legal proceedings or bring to the attention of the judicial authorities violations of data protection provisions, the authorities also have a duty to raise awareness, provide information and educate all players involved (data subjects, controllers, processors etc.). It also allows the authorities to take decisions and impose sanctions. Furthermore, it is recalled that the supervisory authorities should be independent in exercising these tasks and powers." Disponível em <https://rm.coe.int/16808accf8>. Acesso em 18.04.2020.

[46] "Data flows between Parties cannot be prohibited or subject to special authorisation as all of them, having subscribed to the common core of data protection provisions set out in the Convention, offer a level of protection considered appropriate. One exception exists: when there is a real and serious risk that such transfer would lead to circumventing the provisions of the Convention. In the absence of harmonised rules of protection shared by States belonging to a regional international organisation and governing data flows (see for instance the data protection framework of the European Union), data flows between Parties should thus operate freely. Regarding transborder flows of data to a recipient that is not subject to the jurisdiction of a Party, an appropriate level of protection in the recipient State or organisation is to be guaranteed. As this cannot be presumed since the recipient is not a Party, the Convention establishes two main means to ensure that the level of data protection is indeed appropriate; either by law, or by ad hoc or approved standardised safeguards that are legally binding and enforceable (notably contractual clauses or binding corporate rules) , as well as duly implemented." Disponível em <https://rm.coe.int/16808accf8>. Acesso em 18.04.2020.

decorrentes da ausência de salvaguardas adequadas; (ii) os interesses específicos do titular dos dados exijam no caso em concreto e (iii) interesses legítimos prevalecentes, como nos casos de interesses públicos, previstos em lei e que configurem medida proporcional e necessária para uma sociedade democrática.

Por fim, diferente do silêncio sobre o conceito de *tratamento de dados pessoais* das Diretrizes de 1980, a Convenção 108 definiu o conceito de tratamento de dados pessoais como sendo qualquer operação realizada com os dados, como coleta, armazenamento, preservação, alteração, recuperação, divulgação, disponibilização, apagamento, destruição ou realização de operações lógicas ou aritméticas em tais dados. Ressalta-se, contudo, que sua aplicação se destina aquelas atividades cujo tratamento dos dados é automatizado ou quando os dados são coletados para tanto.

Assim como as Diretrizes de 1980, pouco contribui para a conceituação do que significa transferir dados entre fronteiras.

2.3.3 A harmonização de regras de proteção de dados pessoais

Conforme apontado ao longo deste capítulo, é possível perceber que as Diretrizes de 1980 e a Convenção 108 buscavam a harmonização de regras domésticas de proteção de dados pessoais por meio da soma da (i) padronização dos conceitos e princípios jurídicos estipulados no texto das Diretrizes e da Convenção, (ii) autorização de restrições à exportação dos dados a outros países membros em casos específicos e delimitados e (iii) garantia de proteção do nível adequado nos casos de países não signatários.

Com isto em vista, os países passam a assegurar que independente do território do tratamento dos dados pessoais, as mesmas garantias de proteção dos dados e da privacidade serão asseguradas às atividades de tratamento. Dentre os objetivos da harmonização, cita-se a necessidade de evitar os paraísos de tratamento de dados pessoais, os quais são vistos como localidades em que os agentes de tratamento desviam suas atividades para contornar regras locais mais restritivas.

Ainda nesse sentido, Kuner (2009, p. 308) elabora que os padrões internacionais de proteção de dados pessoais contribuem tanto para se evitar lacunas na proteção dos dados entre jurisdições quanto para facilitação do fluxo de dados entre fronteiras[47]. No primeiro caso, aponta-se que a falta de cobertura regulatória sobre o tema cria lacunas na proteção conferida ao dado. No segundo caso, aponta-se que a harmonização de regras facilita o tratamento de banco

[47] "Two main rationales have been advanced for the drafting of international data protection standards: (i) Avoidance of gaps in data protection. The lack of harmonized standards for data protection around the world, and the lack of any data protection legislation in most States, create risks for the processing of personal data. (ii) Facilitation of global data flows. A growing number of data-bases are made accessible globally on the Internet, meaning that the same data processing may be subject to a large number of differing data protection standards, which creates substantial compliance burdens and uncertainty for business." (KUNER, 2009, p. 308).

de dados dispostos na internet, por exemplo, os quais estão submetidos a uma pluralidade de padrões distintos, impondo ônus de conformidade e incerteza para condução dos negócios[48].

A capacidade de harmonização de regras na área de proteção de dados pessoais e privacidade pode se dar por meio de adoção de certos instrumentos que variam em relação à sua forma de criação, tempo, obrigatoriedade e agentes participantes Kuner (2009). Uma primeira possibilidade seria a harmonização por meio de convenções multilaterais. Nesse caso, argumenta-se pela possibilidade de se tratar o tema no âmbito de discussão das organizações internacionais, por meio de suas agências especializadas, como a Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO)[49] e a União Internacional de Telecomunicações (UIT)[50], da Organização das Nações Unidas (ONU) ou, ainda, no âmbito das discussões para negociação que ocorrem na Organização Mundial do Comércio (OMC)[51], a partir das regras contidas no Acordo Geral sobre Comércio de Serviços (GATS)[52].

Para além desta, outras possibilidades poderiam conduzir a harmonização de regras por meio de instrumentos como (ii) convenções regionais e tratados, como é o caso dos padrões de proteção de dados estipulados pelos países membros da APEC e a já mencionada Convenção 108; (iii) lei-modelo (*model laws*); (iv) padrões técnicos não vinculativos; (v) diretrizes internacionais,

48 "The primary motivation for the harmonization of laws has been described as 'to reduce the impact of national boundaries', which fits well with the motivation of many advocates of an international data protection framework to facilitate the flow of personal data around the world."(KUNER, 2009, p. 308).

49 "A UNESCO no mundo e no Brasil. A Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) foi criada em 16 de novembro de 1945, logo após a Segunda Guerra Mundial, com o objetivo de garantir a paz por meio da cooperação intelectual entre as nações, acompanhando o desenvolvimento mundial e auxiliando os Estados-Membros – hoje são 193 países – na busca de soluções para os problemas que desafiam nossas sociedades. É a agência das Nações Unidas que atua nas seguintes áreas de mandato: Educação, Ciências Naturais, Ciências Humanas e Sociais, Cultura e Comunicação e Informação." Disponível em: <https://nacoesunidas.org/agencia/unesco/>. Acesso em: 18.04.2020.

50 "A UIT é a Agência do Sistema das Nações Unidas dedicada a temas relacionados às Telecomunicações e às Tecnologias da Informação e Comunicação (TIC). Ao longo dos seus 154 anos de existência, a UIT tem coordenado o uso global compartilhado do espectro de radiofrequência, promovido a cooperação internacional na área de satélites orbitais, trabalhado na melhoria da infraestrutura de telecomunicações junto a países em desenvolvimento, estabelecido normas mundiais para prover interconexão entre vários sistemas de comunicação, além de dedicar especial atenção a temas emergentes mundiais tais como mudanças climáticas, acessibilidade e fortalecimento da segurança cibernética." Disponível em <https://nacoesunidas.org/agencia/uit/>. Acesso em: 18.04.2020.

51 "There are a number of ways of looking at the World Trade Organization. It is an organization for trade opening. It is a forum for governments to negotiate trade agreements. It is a place for them to settle trade disputes. It operates a system of trade rules. Essentially, the WTO is a place where member governments try to sort out the trade problems they face with each other." Disponível em <https://www.wto.org/english/thewto_e/whatis_e/whatis_e.htm>. Acesso em: 18.04.2020.

52 "The GATS is the first and only set of multilateral rules and commitments covering Government measures which affect trade in services. It has two parts—the framework agreement containing the rules, and the national schedules of commitments in which each Member specifies the degree of access it is prepared to guarantee for foreign service suppliers. The GATS covers all services with two exceptions—i.e. services provided in the exercise of governmental authority and, in the air transport sector, air traffic rights and all services directly related to the exercise of traffic rights. Notwithstanding this very broad scope, the Agreement and the negotiations taking place under it are one of the least controversial areas of current work in the WTO. This is because of its remarkable flexibility, which allows Governments, to a very great extent, to determine the level of obligations they will assume." Disponível em <https://www.wto.org/english/tratop_e/serv_e/gats_factfiction4_e.htm>. Acesso em: 18.04.2020

recomendações e códigos de conduta; (vi) políticas de padrões não vinculativos; (vi) guias legislativos e instrumentos para o setor privado. Abaixo, segue uma tabela relacionando cada possibilidade de harmonização e sua respectiva explicação, tendo como base direta o artigo de Kuner (KUNER, 2009):

Tabela 3 – Explicação de papeis de organizações e instrumentos internacionais segundo Kuner (2009)

Instrumentos de harmonização	**Explicação**
Convenções multilaterais	Adoção de uma Convenção multilateral sobre proteção de dados pessoais a qual, segundo sugere o autor, poderia ser elaborada pela Comissão de Direito Internacional (corpo de especialistas estabelecido pela Assembleia Geral das Nações Unidas em 1947). Outra possibilidade seria basear regras globais de proteção de dados pessoais no âmbito de negociação da Organização Mundial do Comércio - OMC, a partir das regras contidas no Acordo Geral sobre Comércio de Serviços - GATS. Porém, alguns problemas são levantados quando se discute proteção de dados dentro da OMC, como: (i) o foco do GATS está na liberalização do comércio e seria questionável se no âmbito da OMC o tema poderia ser endereçado como um direito fundamental; (ii) o GATS especificamente prevê a regulação sobre proteção de dados pessoais como exceção à aplicação das regras do direito do comércio internacional. Por fim, outras duas possíveis organizações internacionais seriam a Organização das Nações Unidas para a Educação, a Ciência e a Cultura - UNESCO ou a União Internacional de Telecomunicações - UIT. Porém, como são organizações especializadas, enfrentariam dificuldades em criar padrões aplicáveis para as mais diversas áreas, devido à característica transversal das leis de proteção de dados pessoais. O problema, em geral, da harmonização por meio de adoção de Convenção multilateral pelos países estaria no fato de que (i) o tempo de elaboração de uma Convenção é longo, podendo durar cerca de dez anos ou mais; (ii) por se tratar de uma negociação multilateral, o denominador comum dos padrões de proteção de dados pessoais tendem a ser baixos, dado a dificuldade de obtenção de um acordo entre vários Estados; (iii) a incorporação da Convenção no ambiente doméstico poderia passar por adaptações.

Convenções regionais e tratados	É possível destacar dois exemplos existentes nessa categoria de harmonização: (i) a Convenção 108, do Conselho da Europa, adotada em 1980, e (ii) a APEC Privacy Framework, adotada em 2005. No entanto, o autor aponta que a abordagem regional pode gerar alguns entraves para a harmonização internacional visto que a diferença de padrões regionais pode levar a um cenário mais próximo da divisão de padrões do que da harmonização.
Lei-modelo	Esse tipo de instrumento já foi utilizado antes pela Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL). na edição de uma Lei-modelo sobre Comércio Eletrônico em 1996 (MLEC). A finalidade da MLEC é de assistir aos legisladores nacionais apresentando um conjunto de regras internacionais aceitáveis, com o objetivo de remover obstáculos jurídicos e aumentar a previsibilidade jurídica nas transações eletrônicas. Todavia, o processo de implementação no direito doméstico também não garante a harmonização.
Padrões técnicos não vinculativos	Alguns exemplos dessa categoria são padrões técnicos não vinculativos que podem ser adotados por Estados e organizações de forma voluntária, como aqueles criados pela *World Wide Web Consortium* (W3), a Organização Internacional de Normalização (ISO) e a União Internacional de Telecomunicações (UIT). A partir de um ponto de vista prático, o autor aponta que esses padrões podem ser mais efetivos na proteção de dados pessoais do que aqueles criados por leis. No entanto, devem ser vistos com cautela uma vez que podem ser elaborados de forma a avançar interesses de certas indústrias, setores ou companhias. Assim, essa categoria desempenha papel importante para a harmonização de regras dentro do campo, porém é aconselhável que sua implementação ocorra em conjunto com demais instrumentos de harmonização.
Diretrizes internacionais, recomendações e códigos de condutas	Nessa categoria se encaixam exemplos como Diretrizes e Recomendações direcionadas aos países, podendo ter um escopo mais amplo e generalista, conforme as Diretrizes da OCDE de 1980, ou podem apresentar uma abordagem com aplicação setorial, conforme, por exemplo, o Código de Conduta elaborada pelo Organização Internacional do Trabalho (OIT), das Nações Unidas chamado de Proteção dos Dados Pessoais dos Trabalhadores, de 1997.

Políticas de padrões não vinculativos	Grupos que elaboram políticas com padrões voluntários de proteção de dados pessoais que são desenhados para serem aplicados globalmente. A título de exemplo, tem-se o *Global Privacy Standard*, produzido pelo *Working Group* e conduzido pelo *Ontario Information and Privacy Commisioner*[53] e o *Global Network Initiative*[54], elaborado em 2008 por empresas, organizações não governamentais (ONGs) e acadêmicos.
Guias legislativos e instrumentos do setor privado	Guias e Recomendações destinadas a harmonizar legislações nacionais que usam técnicas legislativas diferentes para resolução de um problema. Pode providenciar um conjunto de soluções legislativas para um problema específico de um contexto nacional. Um exemplo desse instrumento é o *Recomendation on the Legal Value of Computer Records* (1985), elaborado pela UNCITRAL. Em relação aos instrumentos do setor privado, o autor cita como exemplo o *Privacy Toolkit*, elaborado pelo *Task Force on Privacy and the Protection of Personal Data of the International Chamber of Commerce* (ICC). Outros exemplos seriam cláusulas contratuais que disciplinem a transferência internacional de dados pessoais e as políticas de privacidade de empresas.

Em relação à escolha de um instrumento internacional com carga jurídica vinculante para os países, é importante ressaltar que ao mesmo tempo que esse instrumento busca garantir o mesmo nível de proteção de dados para todas as Partes, também conta com certas desvantagens, como o tempo de elaboração e aprovação mais longo e obstáculos políticos no caminho. Sobre o assunto, Kuner (2009, p. 315) ainda elabora que experiências de unificação do direito privado mostraram que os Estados tendem a dar menos prioridade na implementação da Convenção no âmbito doméstico, o que torna plausível questionamentos se a elaboração de uma Convenção de regras de proteção de dados levaria à harmonização almejada[55]. Em relação à harmonização de regras por meio das organizações internacionais existentes, o autor aponta para possíveis

[53] Disponível em <http://www.ipc.on.ca/images/Resources/up-gps.pdf>.

[54] "The mission of the Global Network Initiative is to protect and advance freedom of expression and privacy in the ICT industry by setting a global standard for responsible company decision making and by being a leading voice for freedom of expression and privacy rights". Disponível em: https://globalnetworkinitiative.org/team/our-mission/

[55] Each option would have advantages and disadvantages. A binding legal framework would address the problems that have led to the calls for a global framework, namely the lack of data protection standards in many States, and the difficulties that data controllers face in applying differing legal standards to the same data processing. At the same time, a legally binding framework (mostly likely embodied in a multilateral convention) would take much longer to draft and approve than would a non-binding framework, and would also be subject to many political hurdles. Moreover, experience in the unification of private law has shown that States tend to give a low priority to the implementation of such conventions, so that it is questionable whether enactment of a convention would lead to true harmonization. (KUNER, 2009, p. 315).

obstáculos enfrentados pela OCDE, UIT, UNESCO e OMC no processo de harmonização. A OCDE, devido à sua composição cujo número de países membros é limitado. Organizações como UIT, UNESCO e OMC seriam, aos olhos do autor, especializadas demais para assumir tarefa de elaborar um instrumento internacional de proteção de dados cuja aplicação objetiva ser transversal.

Inserida neste contexto, a União Europeia despontou como pioneira e precursora de regulações que visavam a padronização da proteção de dados pessoais entre seus países membros (intrabloco). Dentre elas, convém destacar aqui a revogada Diretiva 95/46/CE, que para além de disciplinar sobre princípios e direitos dos titulares, também criou um regime próprio de transferência internacional de dados pessoais, previsto no Capítulo IV – Transferência de Dados Pessoais a Países Terceiros (então revogado e atualizado pelo Capítulo V do GDPR).

Dentro desse capítulo, sua principal inovação foi a criação do instituto da decisão de adequação, em que se estabelece que, para haver o livre fluxo de dados pessoais entre os Estados Membros da União Europeia e um país terceiro (não membro), deve, este último, ter sido reconhecido com um nível adequado de proteção de dados pessoais pela Comissão Europeia. Como se vê, a Diretiva criou um regime condicional do fluxo de dados entre fronteiras, sendo esta atividade permitida somente após licenças prévias que autorizam a transferência.

A Diretiva previa que a decisão do nível de proteção adequado devia estar baseada em critérios cuja avaliação recaia sob o direito doméstico e os comprometimentos internacionais que o país em avaliação tenha assinado. Em relação ao ambiente doméstico, considerações especiais deviam ser dadas ao Estado de Direito, às leis gerias e setoriais vigentes, às regras profissionais e medidas de segurança que são cumpridas no país[56].

O modelo mais restritivo ao fluxo transfronteiriço de dados pessoais criado pela Diretiva é apontado como uma das principais razões pelas quais os países fora da União Europeia passaram

[56] "Art. 25 – Principles 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination , the rules of law , both general and sectoral , in force in the third country in question and the professional rules and security measures which are complied with in that country. 3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2. 4. Where the Commission finds , under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question . 5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4. 6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals."(PARLAMENTO EUROPEU, 1995, Art. 25).

a adotar leis semelhantes. Para além de ter sido reconhecida como a lei de proteção de dados mais influente[57], a Diretiva ficou marcada pelo seu alcance que se estendeu para fora da União Europeia (efeitos de extraterritorialidade da regulação). Assim, ao condicionar a transferência de dados pessoais para países ou entidades que não protegem os dados pessoais em um nível adequado, conforme as regras dispostas na Diretiva, a União Europeia acabou por incentivar a conformidade internacional de acordo com os seus próprios termos (CUNNINGHAM, 2016).

Conforme exposto por Cunningham (2016, p. 64)[58], se os países estrangeiros e as suas empresas não conseguem realizar o tratamento das informações pessoais dos residentes na União Europeia, o acesso a todo o mercado da União Europeia fica comprometido. Nesse sentido, aponta que a tendência global de conformidade com a Diretiva foi aumentando ao passar dos anos: havia sete novas leis nacionais gerais de privacidade nos anos 1970, dez nos anos 80, dezenove nos anos 90, trinta e duas nos anos 2000 e mais oito surgiram só nos dois primeiros anos da década de 2010[59].

A Diretiva 95/46/CE foi revogada pelo GDPR que, em 2018, entrou em vigor na União Europeia e passou a compor a lista de instrumentos normativos exportadores de padrão de proteção de dados pessoais ao redor do mundo[60]. O GDPR atualizou o instituto da decisão de adequação, trazendo previsão normativa mais específica em relação aos critérios de análise dos países terceiros avaliados. Os critérios do GDPR recaem em três eixos principais: (i) direito doméstico; (ii) requisitos necessários para a autoridade supervisora e (iii) compromissos internacionais. A Comissão Europeia continua sendo o órgão responsável pela decisão de adequação, a qual deve manter o monitoramento constante da parte terceira avaliada e, quando em face de um cenário em que a proteção dos dados pessoais em nível adequado não esteja mais presente, a Comissão pode revogar, alterar ou suspender a decisão.

---

57 (CUNNINGHAM, 2016, p. 427)

58 "One of the key reasons that countries outside the E.U adopted laws similar to the Directive resides in the strictures of the Directive itself. First, most commentators characterize the Directive as the most influential national data protection law. Second, and more importantly, the Directive‘s reach extends outside of the EU containing important provisions concerning international data transfers. By outlawing transfer of personal data to countries or entities that fail to protect personal data in conformity with the Directive, the EU incentivizes international compliance. If foreign countries and their businesses cannot “process” the personal information of EU residents, access to the entire EU market is jeopardized."(CUNNINGHAM, 2016, p. 427).

59 "It is perhaps this panoptic approach that fuels the global trend toward conformity with the Directive. There were seven new national omnibus privacy laws in the 1970s, ten in the 1980s, nineteen in the 1990s, thirty-two in the 2000s, and eight so far in the first two years of this decade. At the current rate of expansion, fifty new laws will emerge in this decade."(CUNNINGHAM, 2016, p. 427).

60 “By the end of the first decade of the 21st century, however, the EU Data protection Directive was coming under different technological, legal and organizational pressures. Multi-national businesses were irritated by diverging interpretations of data protection principles cross Europe, and by the lack of interoperability of basic provisions. The “adequacy regime” had not yielded a significant number of countries to which European organizations could legally transfer personal data. Alternative approaches to legal transfer, based on principles of organizational “accountability” (Guagnin et al., 2012) emerged and became enshrined within a system of Cross Border Privacy Rules (CBPR) legitimated through the Asia Pacific Economic Cooperation (APEC 2005). There was also a urgent desire to “modernize” European data protection to make it relevant for the global networked digital economy, in which social networking services were generating massive volumes of user-generated content, and cloud computing services were rendering geographic borders increasingly irrelevant.” (BENNETT, 2018, p. 240).

2.4 Os fatores do crescimento do fluxo de dados entre fronteiras

Certamente existem diversos fatores que contribuíram para o aumento nas últimas décadas do fluxo de dados entre fronteiras. No entanto, não é a pretensão deste capítulo o exaurimento e apresentação de todos eles. Na verdade, aqui se apresenta três importantes transformações que ocorreram com o surgimento da internet e possibilitaram o formato pela qual esta se apresenta até os dias de hoje: a web, a computação em nuvem e a implementação de cookies (ou tecnologias similares).

A escolha por apresentar os três em detrimento de tantas outras tecnologias que hoje impactam o direito à privacidade e aos dados pessoais está fundamentada em um recorte tanto temporal quanto qualitativo. O primeiro recorte se justifica visto que as preocupações deste trabalho retomam o período de iniciação do debate por meio do estudo do contexto de normas como Diretrizes de 1980, Convenção 108 e Diretiva 95/46/CE, assim como grande parte das decisões de adequação avaliadas no Capítulo 04 desta dissertação ocorreram na década dos anos 2000-2010. Quanto ao recorte qualitativo, este se justifica visto serem tecnologias que possibilitaram o crescimento do mundo digital nos formatos aos quais se apresentam atualmente.

Diante disso, a web, computação em nuvem e cookies contribuíram significativamente para a construção do cenário de intensificação do fluxo de dados pessoais entre fronteiras, destaca-se aqui que (i) a evolução da web (*world wide web*), a partir do desenvolvimento de suas funcionalidades, transformou o usuário da internet em um agente ativo nos modelos de negócio da internet, contribuindo com o aumento massivo de dados gerados e coletados por empresas no mundo online; (ii) os serviços de computação em nuvem, infraestrutura de serviço computacional sob medida, potencializou o surgimento de diferentes formas de exploração econômica pelas empresas e (iii) o modelo de coleta de dados por cookies viabilizou o marketing direcionado na internet, que contribuíram para a forma de capitalização de recursos das empresas e para criação do modelo de negócio na internet conhecido como mercado de preço zero (os dados são a contraprestação do usuário ao acesso a um serviço na internet que não exige contraprestação monetária direta).

Estes três focos de atenção permitem a contextualização de como o avanço da tecnologia digital contribuiu para a facilitação da transferência dos dados entre fronteiras, sendo este último fator importante para o aumento das preocupações sobre privacidade e proteção de dados pessoais que transcendem os assuntos domésticos de um determinado país.

2.4.1 World Wide Web

Em primeiro lugar, convém destacar o que é a web e suas funcionalidades. Trata-se de um software (também conhecido por *web browser*) que permite a navegação na internet. Muito embora a internet e a web sejam ferramentas distintas, é comum haver confusões em relação a cada uma delas. Assim, é relevante esclarecer que enquanto a internet é entendida como algo

maior, a web compõe as funcionalidades da internet.

Em outras palavras, a internet pode ser entendida como um sistema de comunicação entre usuários composto por seis camadas organizadas de forma vertical hierárquica. Assim, conforme Solum e Chung (2003)[61] a internet é dividida do topo para baixo em: (i) camada do conteúdo, que compreende os símbolos e imagens comunicados (como exemplo tem-se o conteúdo, texto, imagem que se vê na tela do computador); (ii) camada de aplicação, que compreende os programas que usam a internet, por exemplo, a web. Trata-se de software que possibilitam que o conteúdo na internet possa ser visualizado/operacionalizado; (iii) camada do transporte, que compreende atividade de quebra dos dados em pacotes e a sua transmissão entre dispositivos; (iv) camada do protocolo de internet, que compreende a administração do fluxo da informação desses pacotes pela internet (responsável pela coordenação do fluxo); (v) camada de ligação, que compreende a conexão da interface entre os computadores dos usuários e a camada física e, por fim, (vi) camada física, que compreende o fio de cobre, cabo ótico, ligações satélites etc[62].

A web, por sua vez, é uma funcionalidade inserida dentro da camada de aplicação - software que possibilita a visualização do conteúdo - e foi desenvolvida, em 1989, por Tim Burners-Lee que almejava criar um espaço comum em que as pessoas pudessem se comunicar por meio de compartilhamento de informação[63,64]. Com seu desenvolvimento, a web chega hoje a ser referenciada em sua versão 4.0, 5.0 e até 6.0. Todas as versões retratam algum desenvolvimento de suas funcionalidades, sendo importante destacar, para os fins desta dissertação, a importância da transformação da web em seus dois primeiros estágios.

[61] A internet dividida em camadas contribui para discussões que pretendem endereçar questões sobre regulação da internet, de forma a conferir obrigações e responsabilidades aos agentes. Principalmente porque ao se definir obrigações e regras de responsabilidades é de extrema relevância que se tenha clareza em relação ao agente e objeto cujas regras se aplicam. Assim, dentro de cada camada pode haver empresas diferentes prestando e desenvolvendo serviços diferentes (que atuam até mesmo em setores diversos).

[62] "What are the layers of the Internet? Viewed as a system of communication between users, the six layers that constitute the Internet are: The Content Layer: The symbols and images that are communicated; The Application Layer: The programs that use the Internet, e.g., the Web; The Transport Layer: TCP, which breaks the data into packets; The Internet Protocol Layer: IP, which handles the flow of data over the network; The Link Layer: The interface between users' computers and the physical layer; and The Physical Layer: The copper wire, optical cable, satellite links, etc. We flesh out this skeletal description in greater detail below. The layers are organized in a vertical hierarchy. When information is communicated via the Internet, the information flows down from the content layer (the "highest"level) through the application, transport, IP, and link layers to the physical layer (the "lowest"level); across the physical layer in packets; and then flows back up through the same layers in reverse order."(SOLUM; CHUNG, 2003, p. 816).

[63] "In 1989, Tim Burners-Lee suggested creating a global hypertext space in which any network-accessible information would be referred to by a single Universal Document Identifier (UDI). The dream behind of the web was to create a common information space in which people communicate by sharing information." (AGHAEI; NEMATBAKHSH; FARSANI, 2012, p. 2).

[64] "Tim Berners-Lee, the architect of the World Wide Web, taught us that the Internet we have is a function of the choices we make about information flows. In 1995, Berners-Lee chose not to patent his work on the World Wide Web because he feared patenting could restrict the free flow of information and limit the universality and openness of the web. Some 20 years later, Berners-Lee continues to fight for this vision of an open Internet. In March 2014, he created a new organization to ensure that the web would remain the 'web we want' – open, free, and neutral." (AARONSON, 2015, p. 1).

Na sua primeira versão somente era possível a leitura na internet pelo usuário (*read-only web*). A funcionalidade da web permitia, portanto, tanto capacidade limitada de divulgação de informações pelas empresas, como margem reduzida aos usuários de participação e contribuição em relação ao conteúdo disponibilizado, diminuindo as possibilidades de interação. Assim, a web 1.0, por ser pouco interativa, era vista como ferramenta em que permitia ao usuário somente funcionalidades como busca pela informação e a capacidade de leitura[65].

A web 2.0, por sua vez, inovou em relação a sua versão anterior por trazer o consumidor ao centro da internet, transformando a experiência pela web em um espaço participativo. Nesta versão, os usuários são capazes de ler e escrever - editar conteúdo ou outras formas de interação - com mais autonomia. Surgem, neste contexto, plataformas como blogs, vídeos, ferramentas de buscas, de suporte à localização (mapas) entre outras. Por meio dessa transformação, a figura do usuário passa a ser vista sob duas óticas ao mesmo tempo: como consumidor e produtor de conteúdo, ou, conforme apontam alguns autores[66], os usuários passam a ser considerados um *prosumer* - termo que busca ressaltar a aproximação dos papeis de produtor e consumidor de conteúdo em uma mesma pessoa. Essa aproximação é feita porque a fronteira de separação entre o papel do provedor de conteúdo na internet e o papel do consumidor de conteúdo se torna fluida a partir das inovações trazidas pela web 2.0. Dessa forma, a delimitação estanque das tarefas e papéis desempenhados por cada agente se torna cada vez mais difícil. Soma-se a tudo isto, as novas capacidades conferidas aos usuários, que passam a ter a capacidade ativa nas atividades de recepção, geração e distribuição de conteúdo ou serviços.

Nesse sentido, em relação aos papéis das empresas que prestam serviço por meio da internet, LEONARDI (2012) explica que a figura do provedor de serviços de internet gera confusões devido à possibilidade de sobreposição da prestação dos serviços por uma mesma empresa, a qual pode, simultaneamente, prestar serviços como provedoras de conteúdo, hospedagem, correio eletrônico ou, ainda, de outros tipos. Vejamos:

> É muito importante compreender que, embora usualmente oferecidas conjunta-

[65] "Web 1.0 was mainly a read-only web. Web 1.0 was static and somewhat mono-directional. Businesses could provide catalogs or brochures to present their productions using the web and people could read them and contacted with the businesses. Actually, the catalogs and the brochures were similarly advertisements in newspapers and magazines and most owners of ecommerce websites employed shopping cart applications in different shapes and forms. The websites included static HTML pages that updated infrequently. The main goal of the websites was to publish the information for anyone at any time and establish an online presence. The websites were not interactive and indeed were as brochure-ware. Users and visitors of the websites could only visit the sites without any impacts or contributions and linking structure was too weak." (AGHAEI; NEMATBAKHSH; FARSANI, 2012, p. 12).

[66] "Driven by advances in technology and the evolving environment, the division between the content providers and content consumers is disappearing as the information consumer is also assuming the role of provider. To describe this phenomenon Tim O'Reilly coined the, well known by now, phrase "Web 2.0". Web 2.0 technologies are already being packaged in a way that enables users not only to receive and to consciously and expressly respond to services, but also generate and distribute new content. Today even the relatively passive act of reception is also recorded as user participation in the world of the Internet that is eventually distilled into anonymous data. The penetration of web services that implicitly process and utilize these data are just another example of the constantly evolving technologies related to the worldwide web." (GIURGIU; BARSAN, 2008, p. 55).

> mente, essas são atividades completamente distintas que podem ser prestadas por uma mesma empresa a um mesmo usuário ou por diversas empresas, separadamente. A confusão é comum em razão de boa parte dos principais provedores de serviços de Internet funcionarem como provedores de conteúdo, hospedagem, acesso e correio eletrônico além de outras ferramentas e recursos adicionais. Porém, a diferença conceitual subsiste e é de fundamental importância para a compreensão da responsabilidade de tais empresas, variável conforme a atividade específica exercida. (LEONARDI, 2012, p. 78)

A evolução da web foi acompanhada de outra inovação tecnológica chamada de computação em nuvem. A ligação existente entre web e computação em nuvem são fatores relevantes na contribuição da expansão do fluxo de dados pessoais entre fronteiras. A seguir, aborda-se o tema da computação em nuvem com mais detalhe.

2.4.2 Computação em nuvem

A definição mais difundida e aceita sobre o que consiste o serviço de computação em nuvem foi desenvolvida pelo Instituto Nacional de Normas e Tecnologia (NIST – *National Institute for Standards and Technology*). Segundo o conceito desenvolvido, trata-se de um modelo em que se permite acesso onipresente, prático e sob demanda a um conjunto compartilhado de recursos de computação configurável[67]. A definição acima foi desenvolvida em 2011, porém já antes disso a computação em nuvem foi reconhecida como um grande marco para a mudança da forma de ser prestar serviço na internet.

Nessa linha, conforme esclarece Picker (2008), a primeira mudança na internet ocorreu com a Web 2.0 e a segunda veio com a computação em nuvem[68]. Com essa transformação, foi possível notar mudanças significativas na forma de armazenamento dos dados. Anteriormente, era necessário que os dados ficassem armazenados no computador ou em algum outro dispositivo como CD, desktop, entre outros. Atualmente, permite-se que, ao invés de se armazenar, por exemplo, os e-mails na memória interna do computador, estes podem ser armazenados remotamente por servidores (PICKER, 2008, p. 3)[69].

---

67 "Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models."(MELL; GRANCE et al., 2011, p. 2).

68 "The term "cloud computing" has entered common usage and has been used to describe a wide range of services offered over the Internet. As such, it can be difficult to differentiate the cloud from other, related Internet and IT services. Some familiar examples help highlight the characteristics that define cloud-based services. Among the cloud services most familiar to consumers are Web-based email (e.g., Gmail), photo hosting sites (e.g., Snapfish), and online financial management programs (e.g., mint. com). What all three of these familiar programs share is that they allow customers to access their data from any Internet-enabled device without installing any files on their computer. Emails, photos, and financial records are stored on the cloud provider's servers, and the provider supplies access to them anytime at the customer's request." (BERRY; REISMAN, 2012, p. 02).

69 "The first shift, often called —Web 2.0, is fundamentally about what we use computers to do. We have moved from creating docu- ments in Microsoft Office to living life online: searching on Google, buying and selling on eBay, watching the newest viral video on YouTube, and hanging out with our friends on mySpace and Facebook. The second shift, often called cloud computing, is a change in the organization of the funda- mental processes of

Mais que isso, o serviço de computação em nuvem pode ser prestado mediante diversas roupagens, variando no modo, extensão e forma do serviço prestado. Dentre os modos do serviço prestado, a computação em nuvem pode abranger infraestrutura como serviço (IaaS – *Infrastructure as a Service*), plataforma como serviço (PaaS – *Platform as a Service*) e software como serviço (SaaS – *Software as a Service*). As definições a seguir são feitas com base no relatório da OCDE publicado em 2012 sobre computação em nuvem, chamado de *Cloud Computing: The Concept, Impacts and the Role of Government Policy*[70].

A infraestrutura como serviço (IaaS) fornece recursos de computação como de processamento e armazenamento de dados e também permite que os usuários aproveitem esses recursos por meio de implementação de capacidades de virtualização própria. Nesse sentido, o serviço é prestado a partir de uma alta flexibilização, em que os contratantes do IaaS podem executar sistemas operacionais e software próprios em cima de hardware oferecidos pela fornecedora de IaaS. Exemplo de prestador desse tipo de serviço é a Amazon Elastic Cloud 2 (EC2)[71], a qual esclarece em seu site que o EC2 foi projetado para facilitar a computação em nuvem na escala da web para desenvolvedores, sendo possível, inclusive, lançar aplicativos sem compromissos antecipados[72].

Nesse sentido, conforme esclarece Cheung e Weber (2015), o provedor de serviço de computação em nuvem oferece infraestrutura de computação básica, como servidores remotos, CPUs, banda de rede e capacidade de armazenamento para clientes e consumidores que são os responsáveis por instalar o sistema operacional e as aplicações. No entanto, medidas de segurança e privacidade para além daquelas relacionadas à infraestrutura ficam à cargo dos clientes[73].

A plataforma como serviço (PaaS) fornece às contratantes plataformas mais estruturadas para implementar aplicações e serviços próprios. Conforme aponta Relatório da OCDE (OECD,

computing—computation and storage. These shifts are not fully independent; the cloud computing shift has some overlap with the Web 2.0 shift. Instead of storing my email on my laptop, I will just out- source storage and store it with Google. I won't have an email product resident on my computer; instead, Google will provide an email service through a Web browser." (PICKER, 2008, p. 3).

70 "This report defines cloud computing as "as a service model for computing services based on a set of computing resources that can be accessed in a flexible, elastic, on-demand way with low management effort." Furthermore, it emphasises that the concept covers a whole cloud service spectrum consisting of infrastructure as a service, platform as a service and software as a service, as well as multiple delivery models including private, public, hybrid and community clouds." (OECD, 2014, P. 4).

71 (OECD, 2014, P. 10).

72 O site ainda disponibiliza testemunho de clientes falando do benefício de se fazer a transição para a nuvem. O engenheiro Tobi Knaup da Airbnb declara que a "Amazon Web Services reconhece as necessidades dos clientes. Se o recurso ainda não existe, provavelmente será disponibilizado em alguns meses. O baixo custo e a simplicidade de seus serviços justificaram facilmente a mudança para a Nuvem AWS" Disponível em <https://aws.amazon.com/pt/ec2/>.

73 "In the first model, that of Infrastructure-as-a-Service (IaaS), the cloud service providers offer basic computing infrastructure such as processing power and/or storage (for example, virtual remote servers, CPU power, network bandwidth and storage capacity) to customers and consumers who are responsible for installing their own operating systems and applications. These providers are often specialized market players that can rely on a physical, complex infrastructure that spans several geographic areas. However, security and privacy provision beyond the basic infrastructure have to be managed bu the users. Examples are Rackspace and Amazon EC2 and S3." (CHEUNG; WEBER, 2015, p. 14).

2014), os usuários dependem de linguagem de programação e outras ferramentas da nuvem para implantar esses aplicativos. Assim, a infraestrutura subjacente como redes ou sistemas operacionais não são controladas pela parte contratante, sendo o provedor de serviço quem gerencia a virtualização das operações. Exemplo dessa categoria de serviço é aquele prestado pela Windows Azure Platform e Google App Engine[74]. Cheung e Weber (2015, p. 14) destacam que neste modelo as responsabilidades pelas medidas de segurança e privacidade são dívidas entre as partes[75].

No software como serviço (SaaS), os usuários possuem acesso direto às aplicações do provedor e, como consequência, possuem a conveniência de não ter que administrar a infraestrutura e recursos da aplicação. Nessa categoria, pode ser incluído desde serviços de e-mail até ferramentas para relacionamento com o cliente, ferramentas de gerenciamento de documentos ou soluções contábeis[76]. Ainda se enquadram como exemplos os serviços do Facebook, Google Maps e Youtube. Neste terceiro modelo, Cheung e Weber (2015, p. 15) destacam que medidas de segurança e privacidade são de responsabilidade principal do provedor de serviço de nuvem. Aos usuários ou clientes é dada a possibilidade de configurar algumas preferências, mas não possuem controle sobre a gerência da infraestrutura e aplicação[77].

Como se vê, a depender do serviço contratado, a divisão de responsabilidade é diferente entre o provedor de serviço de computação em nuvem e o contratante. Enquanto no primeiro modelo (IaaS) o provedor somente é responsável pelos recursos básicos como máquinas, discos e rede e o contratante é responsável pelo gerenciamento do sistema operacional, nos demais modelos (PaaS e SaaS), a infraestrutura, software e dados são de responsabilidade principal dos provedores, pois os contratantes possuem pouco controle sobre as funcionalidades do sistema[78]. A decisão por parte dos contratantes de mover seus serviços para a nuvem (que podem incluir informações de organizações, empresas, dados pessoais entre outros) requer uma análise baseada nos riscos relacionados às opções de segurança e privacidade em jogo[79], sendo importante nessa

[74] Cheung e Weber (2015, p. 14).

[75] "In the second model, that of a Platform-as-a-Service (PaaS), the cloud service providers provide a platform and tools (for example, operating system, database management, security and workflow management, and web servers) to customers and consumers so that they can construct, mainly at market players that use a PaaS to develop and host proprietary application-based solutions to meet in-house requirements or to provide services to third parties. Security and privacy provisions are split between the cloud providers and the cloud users. Examples are Google's App Engine and Microsoft's Windows Azure." (CHEUNG; WEBER, 2015, p. 14).

[76] Cheung e Weber (2015, p. 10).

[77] "Security and privacy provisions are carried out mainly by the cloud service provider. Users do not have control over the cloud infrastructure or applications, except for some administrative or preferential settings." (CHEUNG; WEBER, 2015, p. 15).

[78] "This split of responsibilities has another significant impact on IaaS because the CSPs supply basic resources such as machines, disks and networks, while the users are responsible for the operating system, the software environment necessary to run their application, and the data placed into the cloud computing environment. In contrast, for SaaS or PaaS arrangement, the infrastructure, software and data are the primary responsibility of the CSP as the user has little control over any of these features." (CHEUNG; WEBER, 2015, p. 19).

[79] "The decisions about transitioning organizational data, applications and other resources to a cloud computing environment require an organization to take a risk-based approach to analyzing available security and privacy options. The information technology governance practices of the organization that pertain to the security policies, procedures, implementation, testing, use and monitoring of deployed or engaged services should be extended

análise, verificar questões relacionadas à localização de servidores.

Nesse sentido, é possível notar que a web e a computação em nuvem são duas inovações que foram capazes de criar uma quantidade significativa de dados dos usuários, bem como foram responsáveis por modificar a estrutura organizacional da internet, sendo capaz de deslocar o armazenamento dos dados dos usuários gerados pelo uso de aplicações na internet para centro de dados específicos (PICKER, 2008).

Ainda, conforme desenvolve Antonialli (2010), é possível apontar que a computação em nuvem é hoje um bom exemplo que retrata o problema das disparidades de tratamento da privacidade ao redor do mundo. Isto porque, quando o usuário opta pelo armazenamento de seus dados em servidores acessíveis no mundo todo, eles estão dando informações a empresas que geralmente não estão estabelecidas no seu país. Diante disso, preocupações surgem em relação à escolha de qual concepção de privacidade será aplicada nessa relação visto que se trata de um serviço que transpassa por mais de uma jurisdição. Além do mais, a discussão ainda abrange a tensão já existente no direito de qual lei nacional deve ser aplicada a uma relação que passa por diversas jurisdições. Vejamos[80]:

> A computação em nuvem é outro bom exemplo de incerteza de conformidade com a privacidade. Quando os usuários decidem armazenar suas informações em servidores acessíveis em todo o mundo, eles estão entregando seus dados a uma empresa que geralmente não está localizada em seu país de origem. Se seus dados estão armazenados no exterior, qual lei nacional deve governar a questão da privacidade: o local onde o servidor está hospedado ou o país em que o usuário mora? Estes são exemplos que demonstram que este é um debate sem saída. Existe não apenas uma tensão entre privacidade e controle, mas também uma tensão entres os diferentes conceitos jurídicos nacionais de privacidade e a necessidade de cumprir todos eles ao mesmo tempo. (ANTONIALLI, 2010, p. 15) TRADUÇÃO LIVRE

Já quanto aos benefícios de se contratar um serviço de computação em nuvem para a parte contratante, estudos apontam que as pequenas e médias empresas (PMEs) se beneficiam dos serviços na medida em que garantem acesso imediato e sob demanda a recursos de tecnologia da informação sem a necessidade de despesas de capital próprio em hardware e software[81]. Nessa linha, contratantes de computação em nuvem não precisam fazer investimentos iniciais

to include the use of the cloud computing environment. When shifting risk form locally managed servers and services to the cloud, one should not forget the key areas of security concern, that is, confidentiality (the data should not be exposed, exploited or leaked), integrity (the data should be correct, attestable and not corrupted) and availability (access to the data is not disabled and service is nor denied)." (CHEUNG; WEBER, 2015, p. 20).

[80] "Cloud computing is another great example of privacy compliance uncertainty. When users decide to store their information in servers accessible worldwide, they are giving away their data to a company which is usually not located in their home country. If their data is stored abroad, which national law should govern privacy matters: the one of the place where the server is hosted or the one of the country the user lives in? These are examples which demonstrate that this is a deadlocked debate. There is not only a tension between privacy and control but also a tension between the different national legal concepts of privacy and the necessity to comply with all of them at the same time." (ANTONIALLI, 2010, p. 15).

[81] "The cloud has been changing the way computing is undertaken. Users of cloud computing infrastructure and services do not have to make upfront, capital-intensive investments in Information Technology (IT) infrastructure and software any more but, instead, can pay for computing resources in a pay-as-you go model. Computing is

em infraestrutura e em softwares, pois podem pagar menos pelo serviço prestado por empresas especializadas em um modelo de contratação pré-pago de serviço.

Dessa forma, com o desenvolvimento da web 2.0 e do surgimento do serviço de computação em nuvem, as atividades de coleta, armazenamento e transferência internacional dos dados pessoais passaram a ser executadas com mais facilidade e em grande escala, valorizando ainda mais os dados como ativos. Essa capacidade levantou crescentes questionamentos acerca das externalidades geradas por essas atividades em relação à proteção da privacidade e dos dados pessoais.

2.4.3 Cookies: perfilização e marketing direto

Por fim, também se insere nesse contexto o desenvolvimento de técnicas de rastreamento de usuários na internet por meio de implementação pelos sites de tecnologias de *cookies*, a qual contribuiu para o refinamento de modos de perfilização e direcionamento de marketing online direto.

Para direcionar propaganda aos usuários na internet, as empresas se valem de certas funcionalidades para a coleta dos dados pessoais, bem como para o oferecimento da propaganda em si. Para viabilizar o marketing direcionado destaca-se a implementação: (i) de ferramentas que permitem o rastreamento na internet, como no caso de *cookies* e tecnologias similares para coleta de dados de navegação de usuários com a finalidade de perfilização e direcionamento de marketing direcionado - que se propõe direcionar conteúdo de acordo com as preferências mapeadas - e (ii) de processo de lances em tempo real ("RTB", do inglês *real-time bidding*) de propaganda direcionada, operacionalizados pela internet por meio das adtechs, a qual consiste em termo utilizado para descrever ferramentas que analisam e gerenciam informações de propaganda online, com objetivo central de automatizar o processo e as transações envolvidas[82].

O objetivo de trazer estes dois exemplos não está em exaurir o tema do marketing direcionado, o qual, por si só, demandaria um estudo específico e aprofundado a respeito de suas implicações para o direito à privacidade e aos dados pessoais, bem como sobre o seu modo de operacionalização. Contudo, esta contextualização busca direcionar a leitura para demonstrar mais uma forma de facilitação do fluxo de dados independente de fronteiras, visto a possibilidade

thus deemed to become a utility. This trend is particularly interesting for small and medium enterprises (SMEs), including start-ups, as it allows immediate, on-demand access to information technology resources without the need for capital expenses in hardware and software and thus significantly decreases entry barriers. In addition, many large companies, institutions and governments are examining cloud computing as an important cost saving option that can reduce expenditures on IT infrastructure and services and ongoing maintenance costs." (OECD, 2014, p. 4).

[82] "Adtech is a term used to describe tools that analyse and manage information (including personal data) for online advertising campaigns and automate the processing of advertising transactions. It covers the end-to-end lifecycle of the advertising delivery process, which often involves engaging third parties for one or more aspects of these services, although some advertising is still placed directly between advertisers and publishers." (ICO, 2019b, p. 8).

de acessar sites localizados em servidores em diversas jurisdições diferentes - .br, .pt, .fr, entre outros[83].

Em relação à implementação de cookies, podemos primeiro defini-lo como sendo arquivo de texto em que é feito o download no equipamento do usuário (computador ou smartphone, por exemplo) quando o usuário acessa websites, permitindo o reconhecimento do dispositivo do usuário e armazenamento de algumas informações sobre suas preferências ou ações anteriores[84]. Em geral, um anunciante operando um serviço online utiliza-se de cookies ou tecnologias similares quando o usuário visita o site para coletar informações sobre o dispositivo do usuário, sobre o próprio usuário e sobre a visita feita ao site ou, ainda, sobre seu histórico e perfil de visitas a outros sites. Estas informações são então tratadas com a finalidade de viabilizar a propaganda direcionada.

Na União Europeia, o tema passou a ser regulado de forma específica, por meio da chamada *e-Privacy Directive*, aprovada em 2002, conhecida como Diretiva 2002/58/CE e emendada em 2009, Diretiva 2009/136/CE, que complementam de forma mais específica as regras antes contidas na Diretiva 95/46/CE e no agora atual GDPR. Isto implica dizer que algumas regras mais específicas foram previstas no contexto do direito europeu para a permissão do tratamento de dados pessoais para marketing direcionado em contexto de coleta de dados obtidos por meio de cookies. Este padrão eleva as exigências do denominador comum europeu de *opt-out* para marketing direto e passa a exigir a obtenção do consentimento por meio de *opt-in* aos países membros da União Europeia[85,86].

[83] Diante desse contexto, é importante ressaltar a relevância de estudos cujo escopo está na análise das Políticas de Privacidade e Termos de Uso de sites e aplicativos, uma vez que deveriam ser o instrumento pelo qual as empresas divulgam suas práticas de tratamento de dados para marketing direcionado e implementação e gerenciamento de cookies. Nas Políticas de Privacidade, por exemplo, deveria então constar as práticas da empresa, informando o titular de forma precisa e clara sobre as atividades de tratamento de seus dados, incluindo a forma da coleta, armazenamento, compartilhamentos e transferências que são realizadas, bem como possibilitando, quando cabível, que este consinta com estas práticas ou não.

[84] Trata-se de conceito retirado do site da Autoridade de Proteção de Dados Pessoas do Reino Unido. Conforme dispõe: "A cookie is a small text file that is downloaded onto 'terminal equipment' (eg a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions". Disponível em <https://ico.org.uk/for-organisations/guide-to-pecr/cookies-and-similar-technologies/>.

[85] "(5) Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service." (PARLAMENTO EUROPEU, 2009, Art. 5).

[86] "The Opinion asks advertising network providers to create prior opt-in mechanisms requiring an affirmative action by the data subjects indicating their willingness to receive cookies or similar devices and the subsequent monitoring of their surfing behaviour for the purposes of serving tailored advertising. The Opinion considers that users' single acceptance to receive a cookie may also entail their acceptance for the subsequent readings of the cookie, and hence for the monitoring of their internet browsing. Thus, to meet the requirements of Article 5(3) it would not be necessary to request consent for each reading of the cookie. However, to keep data subjects aware of the monitoring, ad network providers should: i) limit in time the scope of the consent; ii) offer the possibility

A este respeito, o WP29 se posicionou a respeito de diversas obrigações a serem seguidas de forma a cumprir com a transparência e informação ao titular de dados a respeito do uso dos seus dados para criação de perfis para marketing direcionado, estando, dentre elas, a obrigação de informar de maneira clara ao titular sobre (i) os cookies que poderão ser usados para criar perfis, bem como o tipo de informação coletada para a sua construção e que serão usados para a oferta de propaganda direcionada e (ii) que os cookies permitirão a identificação do usuário através de diversos websites[87].

Quanto aos tipos de classificação de cookies, é possível destacar que estes podem ser classificados quanto à sua permanência e quanto à sua origem/titularidade. Em relação à primeira classificação, tem-se os cookies que expiram após encerramento da sessão (*cookies session*) e aqueles cookies denominados de persistentes (*persistent cookies*) porque dependem de uma data estipulada para sua expiração, as quais podem, inclusive, variar no período de expiração em dias, meses ou até anos[88]. Em relação à segunda classificação, os cookies de terceiros são aqueles cookies implementados por um website cujo o nome de domínio do cookies implementado é de outro website - diferente daquele visitado pelo usuário. Assim, é possível que se acesse um website e este implemente no dispositivo do usuário cookies terceiros, cujo controlador dos dados não é o mesmo que possui a titularidade do website visitado[89].

Em relação ao processo de lances em tempo real (RTB), destaca-se suas duas modalidades possíveis: (i) lances que ocorrem diretamente entre anunciante e editores e (ii) lances que se utilizam de ferramentas de *adtech* que intermediam a relação entre anunciante e editores. Nesta última hipótese, conta-se com ferramentas para automatizar as transações de propaganda. O uso de ferramentas de *adtech* pode contribuir, ao menos, com o ganho de eficiência em três sentidos (i) para os anunciantes, ajudam no alcance de novos públicos, aumentando sua velocidade,

to revoke it easily and iii), create visible tools to be displayed where the monitoring takes place. This approach would address the problem of burdening users with numerous notices while ensuring that the sending of cookies and the subsequent monitoring of Internet surfing behaviour for the purposes of serving tailored advertising only takes place with data subjects' informed consent." (WORKING PARTY, 2010, p. 3).

87 "The Article 29 WP would like to recall its Opinion 2/2010, where it is stated that "Ad network providers and publishers must provide information to users in compliance with Article 10 of Directive 95/46/EC. In practical terms, they should ensure that individuals are told, at a minimum, who (i.e. which entity) is responsible for serving the cookie and collecting the related information. In addition, they should be informed in simple ways that (a) the cookie will be used to create profiles; (b) what type of information will be collected to build such profiles; (c) the fact that the profiles will be used to deliver targeted advertising and (d) the fact that the cookie will enable the user's identification across multiple web sites. Network providers/ publishers should provide the information directly on the screen, interactively, if needed, through layered notices. In any event it should be easily accessible and highly visible". (WORKING PARTY, 2011, p. 5). Disponível em <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf>.

88 "A "session cookie" is a cookie that is automatically deleted when the user closes his browser, while a "persistent cookie" is a cookie that remains stored in the user's terminal device until it reaches a defined expiration date (which can be minutes, days or several years in the future)." (WORKING PARTY, 2012, p. 4).

89 "However, from the perspective of browsers, the notion of "third party" is solely defined by looking at the structure of the URL displayed in the address bar of the browser. In this case "third party cookies" are cookies that are set by websites that belong to a domain that is distinct from the domain of the website visited by the user as displayed in the browser address bar, regardless of any consideration whether that entity is a distinct data controller or not." (WORKING PARTY, 2012, p. 4).

reduzindo custos de campanha e permitindo mensuração do sucesso da campanha; (ii) para os editores, ajudam no crescimento da receita ao aumentar o número de potenciais compradores, contribuindo, também, para a valorização do espaço ofertado ao anunciante e ainda ajuda na venda de outros espaços que não seriam vendidos; (iii) para os intermediários, na medida em que ganham receita com a intermediação neste processo de compra e venda de espaço publicitário[90].

O RTB usa *adtechs* para facilitar a compra e venda do inventário de propaganda em tempo real, no instante em que o conteúdo do site está sendo carregado no browser do usuário. Trata-se de um dos tipos de se implementar propaganda online e é aplicado em contexto de conteúdo visual em sites ou apps. Esse tipo de tecnologia também pode ser aplicada em outros canais, como para viabilizar a propaganda em áudio, vídeo streaming e em outdoors (por meio de tecnologias de detecção ou reconhecimento facial). O RTB envolve leilões abertos, apesar de que as tecnologias implementadas também podem ser aplicadas em ambiente de leilões privados (ICO, 2019).

No que toca à importância do RTB para o tema de proteção de dados pessoais e privacidade, podemos citar as práticas que envolvem: (i) perfilização e decisão automatizada; (ii) tratamento de dados pessoais em larga escala (incluindo as categorias especiais de dados); (iii) uso de tecnologias inovadoras; (iv) combinação e correspondência de dados vindos de múltiplas fontes; (v) rastreamento de geolocalização e/ou análise comportamental e (vi) tratamento invisível, desconhecido pelo titular de dados pessoais (ICO, 2019).

Sobre a relação entre informação adequada, financiamento pela indústria online dos serviços digitais gratuitos e sua respectiva aceitação pelos usuários, a ICO (autoridade de proteção de dados pessoais do Reino Unido) contratou a empresa Harris Interactive para realizar pesquisas sobre a publicidade online. Dentre os resultados das pesquisas, ressalta-se que 63% dos 2.300 participantes indicaram achar aceitável que os anúncios financiassem conteúdo gratuito. No entanto, quando receberam explicações de como o RTB funciona, esse valor caiu para 36%[91].

Segundo as orientações emitidas pelo WP29[92], nas *Guidelines on Automated individual decision-making and profiling for the purposes of Regulation n. 2016/679*, adotadas pelo WP29,

[90] "Use of adtech may enable: advertisers to reach new audiences, increase the speed at which an advertisement reaches its audience, reduce the cost of campaigns and make the success of an advertising campaign more measurable; publishers to drive increased revenue by increasing the number of potential buyers for advertising space they want to sell, thereby increasing the value of individual advertising space sold, and selling advertising space that would otherwise not be sold; and intermediaries to make money through providing services to others in the ecosystem such as agencies and publishers, who use their services to purchase and deliver advertising." (ICO, 2019b, p. 8).

[91] "The ICO commissioned Harris Interactive to undertake research into online advertising. 63% of the 2,300 participants indicated they found it acceptable that ads funded free content; however, when they were given an explanation of how RTB works, this fell to 36%." (ICO, 2019b) Disponível em: <https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf>.

[92] Segundo informação do site da Comissão Europeia "O Grupo de Trabalho do Artigo 29.º (GT Art. 29.º) é o grupo de trabalho europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018". Disponível em <https://edpb.europa.eu/our-work-tools/article-29-working-party_pt>.

em 3 de outubro de 2017, a perfilização e decisões automatizadas são também usadas em um número crescente de setores, bem como pelo setor público e privado[93]. O WP29 cita como exemplo de grandes utilizadores desta técnica setores como o bancário, saúde, seguros, marketing e propaganda e ainda prossegue nesta introdução ao tema ao reforçar que a disponibilidade massiva de dados pessoais na internet e a capacidade de encontrar correlações podem permitir que aspectos da personalidade dos indivíduos ou de seus comportamentos, interesses e hábitos sejam determinados, analisados e previsíveis.

Ainda nas orientações do WP29, destaca-se que a capacidade de inferência sobre as pessoas a partir dos dados gerados pode perpetuar estereótipos e a segregação social, causando estigmatização de pessoas em determinadas categorias e possível restrição de escolhas conforme às suas sugestões de preferências. Neste último caso, a delimitação prévia por terceiros do conteúdo a ser disponibilizado ao usuário - a partir de suas preferências mapeadas - podem diminuir a liberdade de escolha dos indivíduos, como, por exemplo, na possibilidade de escolher certos produtos ou serviços (como ocorre no caso de livros, músicas ou os tipos de notícias). Ainda alguns casos a perfilização[94] podem levar a predições equivocadas, como na negativa de prestação de um determinado serviço ou produto de forma discriminatória.

Considerando esses problemas, foram criadas na União Europeia duas obrigações como forma de garantir mais autonomia aos titulares de dados pessoais, como: (i) a necessidade de consentimento para coleta de cookies de marketing e (ii) o direito de explicação da lógica da decisão automatizada. Sobre este último ponto, ao invés de fornecer explicações complexas sobre a lógica matemática, algorítmica ou sobre o aprendizado de máquina por trás do processo de tomada de decisão, a empresa ou outra organização que assim esteja operando deve fornecer informações aos titulares a respeito dos (ii.a) tipos de dados que foram ou serão usados para a perfilização ou para a tomada de decisão automatizada; (ii.b) porque esses dados são considerados pertinentes; (ii.c) como o perfil é usado nas decisões automatizadas; (ii.d) como o perfil é relevante e usado no processo de tomada de decisão.

93 "Profiling and automated decision-making are used in an increasing number of sectors, both private and public. Banking and finance, healthcare, taxation, insurance, marketing and advertising are just a few examples of the fields where profiling is being carried out more regularly to aid decision-making." (WORKING PARTY, 2017, p. 5).

94 "Broadly speaking, profiling means gathering information about an individual (or group of individuals) and evaluating their characteristics or behaviour patterns in order to place them into a certain category or group, in particular to analyse and/or make predictions about, for example, their: ability to perform a task; interests; or likely behaviour." (WORKING PARTY, 2017, p. 5).

3 O REGIME EUROPEU DE TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS

Por meio da implementação do Mercado Único Digital (DGM, sigla em inglês para *Digital Single Market*)[1], a União Europeia busca implementar medidas cujo objetivo é melhorar as condições de competitividade na economia digital eliminando barreiras nacionais[2]. O objetivo da estratégia é encontrar níveis de harmonização de regras entre seus países membros e antecipar certas preocupações consideradas chaves para a competitividade e crescimento econômico do mercado digital, como as questões envolvendo computação em nuvem, big data e internet das coisas. Com isso, pretende-se diminuir as barreiras regulatórias incidentes nos serviços digitais e aumentar o alcance do mercado. Dentre os diversos temas que importam para as medidas de harmonização do DGM estão as regras de proteção de dados pessoais, hoje reguladas pelo GDPR e positivadas como direito fundamental na Carta dos Direitos Fundamentais da União Europeia (CDFUE)[3].

Diante desse tema, a União Europeia, conforme já anunciado neste trabalho, contava já desde 1995 com a Diretiva 95/46/CE que, de fato, protegia a livre circulação dos dados pessoais entre os países membros da União Europeia, diminuindo barreiras regulatórias em seu mercado interno. Contudo, estabelecia regime específico ao regular a transferência de dados pessoais entre os países da União Europeia a países não membros - estes chamados pela Diretiva de terceiros.

---

1 "O Mercado Único Digital visa essencialmente a supressão das barreiras nacionais às transações em linha. O Mercado Único Digital tem por base o conceito de mercado comum, que visa a supressão das barreiras comerciais entre os Estados-Membros com o objetivo de aumentar a prosperidade económica e contribuir para «uma união cada vez mais estreita entre os povos da Europa», e passou a ter por base o conceito de mercado interno, definido como «um espaço sem fronteiras internas no qual é assegurada a livre circulação de mercadorias, pessoas, serviços e capitais». No seguimento da Estratégia de Lisboa, a Estratégia Europa 2020 introduziu a Agenda Digital para a Europa como uma das sete iniciativas emblemáticas, reconhecendo o papel importante que a utilização das tecnologias da informação e das comunicações (TIC) terá de desempenhar se a Europa quiser ver as suas ambições para 2020 coroadas de sucesso. O Mercado Único Digital foi reconhecido como uma prioridade pela Comissão Europeia na sua Estratégia para o Mercado Único Digital (MUD)." Disponível em <http://www.europarl.europa.eu/factsheets/pt/sheet/43/a-ubiquidade-do-mercado-unico-digital>.

2 "A Europa tem as capacidades necessarias para ser líder na economia digital global, mas nao estamos atualmente a aproveitar plenamente todo o seu potencial. A fragmentacao e os obstaculos que nao existem no Mercado Unico fisico estao a impedir a UE de avancar. A eliminacao desses obstáculos dentro da Europa poderia contribuir para um aumento adicional do PIB europeu de 415 mil milhoes de euros. A economia digital pode expandir os mercados e promover melhores servicos a melhores precos, oferecer uma maior escolha e criar novas fontes de emprego. Um Mercado Único Digital pode criar oportunidades para novas empresas em fase de arranque e permitir que as empresas existentes cresçam e tirem partido da escala de um mercado de mais de 500 milhões de pessoas." (COMISSÃO EUROPEIA, 2015, p. 15). Disponível em <https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2015/0192/COM_COM(2015)0192_PT.pdf>.

3 "No que se refere aos dados pessoais e a privacidade, a UE esta empenhada em manter os mais elevados niveis de protecao garantidos pelos artigos 7.o e 8.o da Carta dos Direitos Fundamentais. O Regulamento Geral sobre Protecao de Dados reforcara a confianca nos servicos digitais, uma vez que devera proteger as pessoas no que se refere ao tratamento de dados pessoais por parte de todas as empresas que oferecem os seus servicos no mercado europeu." (COMISSÃO EUROPEIA, 2015, p. 15). Disponível em <https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2015/0192/COM_COM(2015)0192_PT.pdf>.

Como a então Diretiva 95/46/CE dependia de transposição pelo direito nacional do país membro da União Europeia, ainda permaneciam as chances de fragmentação das regras sobre proteção de dados pessoais, frustrando as tentativas de harmonização de regras no mercado único. Nesse sentido, Voigt e Bussche (2017, p. 2) apontam que uma atividade de tratamento podia ser considerada ilegal em um Estado Membro, mas permitida em outro, causando diferenças na sua implementação. O GDPR surge como instrumento capaz de superar esta fragmentação visto ter aplicação direta, sem necessidade de transposição para o direito nacional. Sobre isto, explica Voigt e Bussche (2017, p. 2)[4]:

> Diretivas da União Europeia não são diretamente aplicáveis em todos os Estados Membros da União Europeia, mas têm que ser transpostas ao direito nacional. Assim, exigem medidas de implementação em cada Estado Membro. A Diretiva de proteção de dados não correspondeu aos seus objetivos e não conseguiu alinhar o nível de proteção de dados na UE. Diferenças legais surgiram em consequência dos atos de implementação adotados pelos Estados Membros. Atividades de tratamento de dados permitidas em um membro da UE poderia ser ilegal em outro, no que diz respeito à execução específica do tratamento de dados. (VOIGT; BUSSCHE, 2017, p. 2) TRADUÇÃO LIVRE

Assim como buscava implementar a Diretiva, o GDPR contribui para a padronização de regras e a garantia do livre fluxo de dados pessoais entre seus Estados Membros. Diante disso, é possível destacar que ambos instrumentos normativos foram redigidos de forma a garantir a livre circulação de dados pessoais dentro da União Europeia, sendo proibido que seus Membros criem restrições ao fluxo dos dados pessoais com fundamento na proteção dos direitos da privacidade e proteção de dados pessoais. Como se vê na tabela a seguir, a livre circulação de dados pessoais entre os membros da União Europeia é estabelecida como objetivo tanto da revogada Diretiva como do atual GDPR, os quais promovem a livre circulação dos dados no interior da União e proíbem que os Estados se valham da restrição por razões de proteção dos dados pessoais.

Tabela 4 – Comparação entre Diretiva e GDPR

Diretiva 95/46/EC	**GDPR**
Artigo 1º Objecto da directiva (...) 2. Os Estados-membros não podem restringir ou proibir a livre circulação de dados pessoais entre Estados-membros por razões relativas à protecção assegurada por força do nº 1.	Artigo 1º Objeto e objetivos (...) 3. A livre circulação de dados pessoais no interior da União não é restringida nem proibida por motivos relacionados com a proteção das pessoas singulares no que respeita ao tratamento de dados pessoais.

[4] "European directives are not directly applicable in all EU Member States but have to be transposed into national law. Thus, they require implementation measures in each EU Member State. The Data Protection Directive did not live up to its objectives and failed to align the level of data protection within the EU. Legal differences arose as a consequence of the implementing acts adopted by the various EU Member States. Data processing activities that were allowed in one EU Member State could be unlawful in another one with regard to the specific execution of data processing." (VOIGT; BUSSCHE, 2017, p. 2).

No entanto, os dados que saem do território da União Europeia para países considerados terceiros (não membros) não contam com o mesmo regime de livre circulação de dados pessoais. Este tratamento diferenciado se justifica visto a ausência de garantia de que o país terceiro possui um regime de nível de proteção adequado ao tratamento dos dados pessoais segundo os denominadores comuns de proteção europeus. Por conta disso, a Diretiva disciplinou este tema em seu Capítulo IV – Transferência de dados pessoais para países terceiros, que foi então substituído pelo GDPR em seu Capítulo V – Transferência de dados pessoais para países terceiros ou organizações internacionais.

As regras de transferência contidas no GDPR expandem o regime anterior da Diretiva com destaque para três pontos relacionados aos (i) critérios objetivos e subjetivos aplicáveis às decisões de adequação; (ii) a previsão normativa das hipóteses de salvaguardas adicionais e (iii) a previsão normativa das hipóteses excepcionais que justificam a transferência. A seguir, explica-se com mais detalhes.

No que se refere ao instituto da decisão de adequação, o GPDR elenca critérios mais específicos para a análise a ser conduzida pela Comissão Europeia, bem como expande, em sua texto normativo, os atores sujeitos à verificação de adequação, os quais podem ser países terceiros, seus territórios ou regiões específicas e organizações internacionais. Em relação às salvaguardas adicionais, o GDPR prevê que se aplicam em contexto em que não há uma decisão de adequação e deve ser adotada na relação entre importador e exportador de dados pessoais. Por fim, o GDPR estipula hipóteses específicas que autorizam a transferência entre países, porém as condicionam como excepcionais, sendo aplicáveis nos casos em que não se tem a garantia da primeira nem da segunda hipótese.

Abaixo seguem duas tabelas. A primeira esclarecendo o modelo anterior da redação da Diretiva e a segunda esclarece o atual modelo de redação de transferência internacional de dados pessoais contidos no GDPR. A tabela a seguir, a respeito da Diretiva, esclarece em camadas (i) o instituto da decisão de adequação, seguido das previsões de (ii) hipóteses específicas autorizadoras da transferência e, por fim, (iii) do modelo de cláusula contratual adequada e cláusula contratual padrão, com competência para aprova-las, respectivamente, a Autoridade Nacional e a Comissão Europeia.

Tabela 5 – Modelo da Diretiva e explicação do regime de transferência

Diretiva 95/46/EC	**Explicação**
Previsão do instituto da decisão de adequação (art. 25 da Diretiva).	Neste caso, a avaliação recaia sobre um país terceiro. Tratava-se de decisão a ser proferida pela Comissão Europeia, cujos pontos de avaliação abordavam critérios aplicáveis ao direito doméstico -podendo envolver uma determinada legislação ou compromissos internacionais - e às circunstâncias da transferência.
Previsão de hipóteses específicas autorizadoras da transferência internacional de dados pessoais (art. 26, (1), a-f da Diretiva).	Trata-se de seis hipóteses, aplicadas em derrogação ao art. 25, cuja transferência poderia ser fundamentada em razão de (i) consentimento inequívoco; (ii) execução do contrato entre o titular e o responsável do tratamento ou, ainda, relacionada a diligências prévias à formação do contrato decididas a pedido do titular; (iii) execução de contrato celebrado ou para a celebração de contrato entre o responsável pelo tratamento e um terceiro no interesse da pessoa em causa; (iv) proteção de um interesse público ou para declaração, exercício ou defesa de um direito em processo judicial; (v) proteger interesses vitais da pessoa em causa; (vi) realizada a partir de um registro público, que se destina à informação geral e se encontre aberto à consulta pelo público ou por qualquer pessoa que possa provar um interesse legítimo.

Cláusulas contratuais adequadas e cláusulas contratuais padrão (art. 26, (2), (3), (4) da Diretiva).	O Estado Membro pode autorizar uma transferência ou um conjunto de transferências de dados pessoais para um país terceiro (com nível de adequação não reconhecido) desde que o responsável pelo tratamento apresente garantias suficientes de proteção da vida privada e dos direitos e liberdades fundamentais das pessoas, assim como do exercício dos respectivos direitos. Tais garantias podem resultar de cláusulas contratuais adequadas. Nestes casos, os Estados Membros deveriam informar à Comissão a respeito das autorizações concedidas. Em relação à Comissão, cabia a esta a competência de aprovar cláusulas contratuais padrão, devendo os Estados Membros tomar as medidas necessárias para dar cumprimento à decisão da Comissão.

Apesar da estrutura assim disposta da redação da Diretiva a respeito das regras de transferência de dados pessoais a países terceiros, em 3 de junho de 2003, o WP29 reconheceu as normas corporativas globais como medida cabível dentro da hipótese de garantias adequadas do artigo 26 (2). O reconhecimento se deu por meio do documento intitulado *Working Document: transfer of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*[5].

Adicionalmente, o WP29 em dois documentos aprovados em 1998 e em 2005 também esclareceu que as derrogações (as hipóteses específicas ilustradas na tabela acima) foram desenhadas para lidar com um número limitado de situações em que se aplicam como exceção à adequação e devem, portanto, ser interpretadas de forma restrita. Os documentos são, respectivamente, (i) *Working Document 12/2001: transfers of personal data to third countries: Applying Articles 25 and 26 of the Data Protection Directive* e (ii) *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC*. Neste último, o WP29 explica de forma detalhada o contexto de aplicação das hipóteses específicas de aplicação do artigo 26 (1) da revogada Diretiva.

[5] "Finally, the Article 29 Working Party would like to reiterate that adducing sufficient safeguards within the meaning of Article 26 (2) is a broad concept that certainly includes contractual solutions and binding corporate rules but may also cover other situations not dealt with by this paper which data protection authorities can also consider suitable for the granting of authorisations. This working document, nevertheless, has reviewed the application of Article 26 (2) of the Directive in the particular case of the binding corporate rules." (WORKING PARTY, 2003, p. 6).

Em relação ao regime contido no GDPR, destacam-se as três grandes possibilidades de transferência internacional de dados pessoais que introduzem na estrutura da norma as orientações proferidas até então pelo WP29. Assim, a primeira se vale do livre fluxo de dados pessoais a partir de uma decisão de adequação, após reconhecimento pela Comissão Europeia do nível adequado de proteção. Conforme se vê, trata-se de hipótese já prevista no modelo anterior, porém o GDPR expandiu seu critério de análise sobre os critérios de avaliação e o terceiro avaliado.

A segunda possibilidade trata das salvaguardas adicionais que se aplicam no contexto de não reconhecimento de nível adequado pela Comissão Europeia em relação ao país terceiro. Nesta situação, as salvaguardas adicionais buscam garantir o nível adequado do tratamento dos dados na relação importador-exportador dos dados pessoais. Trata-se de implementação de mecanismos privados, como cláusulas contratuais padrão (SCCs), normas corporativas globais (BCRs) e selos, certificação e códigos de conduta.

A terceira possibilidade trata de hipóteses que devem ser usadas mediante um regime de aplicação excepcional. Em outras palavras, devem ser consideradas nos casos em que não se encontra uma decisão de adequação, nem as salvaguardas estejam asseguradas e tenham sido implementadas pelos agentes de tratamento (importador e exportador de dados pessoais). Diante disso, as hipóteses podem, a partir de situações excepcionais e não corriqueiras, ser utilizadas para dar fundamento à transferência. A tabela a seguir sistematiza essas três grandes possibilidades.

Tabela 6 – Modelo do GDPR e explicação do regime de transferência

GDPR	**Explicação**
Decisão de adequação (art. 45 (1) a (9) do GDPR)	Destinado a um país terceiro, território ou um ou mais setor de um país terceiro ou organização internacional que proporcionem grau de proteção de dados pessoais adequado. Trata-se de decisão a ser proferida pela Comissão Europeia, cujos critérios recaem em pontos específicos referentes ao (i) direito doméstico; (ii) requisitos necessários para a autoridade supervisora e (iii) compromissos internacionais.

Salvaguardas (art. 46 (1) a (5) do GDPR)	O exportador pode transferir dados pessoais a países ou organizações terceiras quando os agentes de tratamento providenciarem salvaguardas apropriadas e sob a condição de medidas que cumpram com os direitos dos titulares e ofereçam remédios judiciais efetivos aos titulares de dados. Os instrumentos previstos são: (i) cláusulas-padrão contratuais, que podem ser adotadas pela Comissão ou pela Autoridade Nacional; (ii) normas corporativas globais, aprovadas pela Autoridade Nacional competente e (iii) mecanismos de certificação e código de condutas.

Exceções (art. 49 (1) a (6) do GDPR)	Na ausência de uma decisão de adequação ou de salvaguardas apropriadas, pode ocorrer a transferência internacional de dados quando em face das seguintes condições: (i) consentimento explícito, depois de informado sobre os riscos devido à ausência de uma decisão de adequação e salvaguardas apropriadas; (ii) necessária para execução de um contrato entre o titular de dados e o responsável pelo tratamento ou para a implementação de medidas pré-contratuais tomadas a pedido do titular de dados; (iii) necessária para celebração ou execução de um contrato celebrado no interesse do titular dos dados entre o responsável pelo tratamento e outra pessoa natural ou jurídica; (iv) necessária para razões importantes de interesse público; (v) a transferência é necessária para o estabelecimento, exercício ou defesa de ações judiciais; (vi) necessária para proteger interesses vitais do titular dos dados ou de outras pessoais, quando o titular está física ou legalmente incapaz de oferecer o consentimento; (vii) quando a transferência é efetuada a partir de um registro que visa fornecer informações ao público e está aberto a consulta pelo público em geral ou por qualquer pessoa que possa demonstrar um interesse legítimo, de acordo com a legislação da União e Estados Membros.

Neste cenário, a transferência internacional de dados pode ocorrer, sobretudo, quando observadas as regras contidas no Capítulo V – Transferência de dados pessoais a países terceiros ou organizações internacionais do GDPR. Este capítulo se incumbe da tarefa de explicar a decisão de adequação, instituto jurídico sob análise nesta dissertação e que está inserido normativamente dentre uma das possibilidades que autorizam a transferência internacional de dados pessoais.

Destaca-se que, uma vez reconhecido com nível adequado de proteção, o terceiro passa a

dispor de um regime de circulação de dados parecido com aquele aplicado aos Estados Membros da União Europeia, o qual passa a ocorrer sem a necessidade de implementação de outras salvaguardas adicionais ou por meio de hipóteses específicas que autorizam a transferência. Trata-se da garantia de implementação do livre fluxo de dados pessoais.

3.1 Decisão de adequação: os primeiros documentos sobre o tema

Como explicado, a primeira forma de se garantir o livre fluxo de dados pessoais, sem necessidade das partes adotarem mecanismos adicionais de garantias do nível adequado da proteção dos dados exportados, é por meio da decisão de adequação (regulada pelo artigo 45 (1) a (9) do GDPR e, antes da entrada em vigor do GDPR, pelos artigos 25 da Diretiva 95/46/CE). Nessa transição, os critérios objetivos e subjetivos relacionados à avaliação da adequação foram expandidos. A seguir, destaca-se a expansão referente a cada um dos critérios.

No que se refere à ampliação do critério subjetivo, a redação atual do GDPR passa a contemplar expressamente a possibilidade de além do país terceiro avaliado, se reconhecer também a adequação em relação a um território ou um ou mais setor de um país terceiro ou organização internacional. Sobre isto, apesar da Diretiva não conter texto expresso possibilitando adequação referente a um setor específico, isto já veio sendo feito pela Comissão Europeia ao avaliar, na decisão de adequação, o nível de proteção referente a uma lei em específico (caso do Japão e do Canadá, por exemplo). Estas decisões possuem fundamento no artigo 25, (5) da Diretiva, o qual previa a possibilidade de um país terceiro assegurar nível adequado em virtude de sua legislação interna e de compromissos internacionais assumidos.

Já no que toca à ampliação dos critérios objetivos, destaca-se que o GDPR passa a contemplar critérios mais específicos e detalhados a respeito dos temas necessários para a adequação de um terceiro. A Diretiva previa critérios como a necessidade de se avaliar as circunstâncias da transferência (natureza do dado, finalidade, duração do tratamento), o país de origem e destino e as respectivas regras do direito doméstico (regras profissionais e medidas de segurança, gerais e setoriais). O GDPR, por sua vez, GDPR dispõe de um conjunto de critérios que podem ser divididos em (i) direito doméstico; (ii) requisitos necessários para a autoridade supervisora e (iii) compromissos internacionais.

Quanto à avaliação do direito doméstico do país analisado, segundo dispõe o artigo 45 (2) (a) do GDPR, trata-se de verificar as condições relacionadas ao Estado de Direito, o respeito aos direitos humanos e liberdades individuais, a legislação relevante, geral e setorial (incluindo segurança pública, defesa, segurança nacional, direito penal e acesso por autoridades públicas aos dados pessoais) e a sua respectiva implementação, regras de proteção de dados pessoais, regras profissionais e medidas de segurança, regras de transferência subsequente de dados para outros países ou organização internacional, jurisprudência, direito dos titulares de dados e remédios

judiciais e administrativos disponíveis aos titulares cujos dados estão sendo transferidos.

Quanto à avaliação da autoridade supervisora, segundo dispõe o artigo 45 (2) (b) do GDPR, trata-se de compreender se as autoridades supervisoras do país gozam de certas prerrogativas de forma a desempenhar função de investigação e intervenção adequada às atividades de tratamento. Assim, dentre outras exigências, requer-se que o país ou a organização internacional tenham uma autoridade de proteção de dados independente, com poder de investigação e intervenção de forma a garantir a conformidade com as regras de proteção de dados pessoais. A autoridade também tem papel importante para que possa desempenhar função de cooperação com as autoridades dos Estados Membros da União Europeia.

Por fim, a avaliação dos acordos e compromissos internacionais, segundo dispõe o artigo 45, (2) (c) do GDPR, tem enfoque nos tratados e convenções assinados pelo país, bem como na sua participação em sistemas multilaterais ou regionais em que faça parte, com especial atenção àqueles que disciplinam sobre proteção de dados pessoais.

Como já ressaltado ao longo desta dissertação, a Comissão Europeia é o órgão responsável pela decisão de adequação, tanto sob a orientação da Diretiva como sob a do GDPR, a qual tem a prerrogativa de monitorar os andamentos do tema no país terceiro avaliado, de modo que, em face de qualquer mudança significativa, a Comissão pode revogar, alterar ou suspender a decisão em casos em que o cenário de proteção dos dados pessoais não apresente mais um nível adequado. Nesse processo de tomada de decisão, a Comissão Europeia contou, ao longo dos anos, com as diretrizes e opiniões emitidas pelo WP29, o qual deu suporte por meio de dois eixos importantes (i) emissão de pareceres a respeito do país terceiro avaliado, o qual são somente referenciados na decisão de adequação, sem qualquer exploração do relatório emitido pelo WP29 no seu conteúdo pela Comissão Europeia nas decisões proferidas e (ii) por meio documentos que serviram como diretrizes para o processo metodológico de se avaliar o sistema jurídico de um país terceiro. Destaca-se aqui aqueles emitidos nos primeiros anos da vigência da Diretiva - 1997 e 1998 - cujo objetivo era trazer balizas para o processo de avaliação de um país terceiro pela Comissão Europeia. Atualmente, sob o âmbito de aplicação do GDPR, este papel é desempenhado pelo atual *European Data Protection Board* (EDPB).

Os documento balizadores publicados pelo WP29 são: (i) "Primeiras orientações sobre a transferência de dados pessoais a países terceiros – possíveis caminhos para avaliar a adequação ("WP4")", adotado em 26 de junho de 1997; (ii) "Julgando a autorregulação da indústria: quando a autorregulação faz contribuição significativa ao nível de proteção de dados pessoais de um país terceiro? ("WP7")", adotado em 14 de janeiro de 1998; (iii) "Visão preliminar sobre o uso de cláusulas contratuais no contexto de transferência de dados pessoais a países terceiros", adotado em 22 de abril de 1998; (iv) "Transferência de dados pessoais para países terceiros: aplicando artigo 25 e 26 da Diretiva 95/46/EC (WP12)", adotado em 24 de julho de 1998.

A seguir, a análise recai sobre os documentos (i) e (ii), visto que versam sobre a aplicação da decisão de adequação. Em relação aos dois restantes, estes não serão aprofundados porque

saem do escopo de análise desta dissertação. O (iii) porque traz observações a respeito da implementação das cláusulas contratuais e o (iv) porque no que se refere ao artigo 25, repete o que já disposto no WP4 e no que se refere ao artigo 26, este versa sobre conteúdo que diz respeito à aplicação das cláusulas contratuais como hipótese autorizadora da transferência, o que não é o objeto direto de estudo desta dissertação. Diante disso, seguem observações a respeito dos dois primeiros documentos.

3.1.1 Os critérios materiais e procedimentais de um sistema regulatório

O primeiro documento (WP4) buscou dar direcionamentos à interpretação do artigo 25 parágrafos (1) e (2) da Diretiva. Conforme destacado, o WP29 ressalta dificuldades inerentes ao processo de avaliação de um país terceiro, visto a complexidade de se avaliar sistemas jurídicos. No que se refere ao tema da proteção de dados, o WP29 destaca a dificuldade de se ter um sistema uniforme cuja proteção dos dados pessoais é a mesma para todos os setores da economia. Como é possível notar, esta preocupação está relacionada ao modelo europeu de proteger o tema da privacidade por meio de uma legislação geral[6].

Como exemplo desta complexidade, por exemplo, o WP29 menciona que em muitos países há leis de proteção de dados pessoais aplicáveis às atividades de tratamento desenvolvidas pelo setor público, porém não são estendidas ao setor privado. Mais especificamente, destaca-se como exemplo neste sentido o caso dos Estados Unidos, em que a situação se mostra ainda mais complexa visto que se trata de país cujas leis de proteção de dados são destinadas a temas específicos (por exemplo, saúde, financeiro entre outros) e ainda possui um sistema federativo em que permite diferenças de proteção entre os Estados a respeito dessas normas.

A preocupação referente à possíveis diferenças entre setores da economia no tratamento de dados pessoais deve ser considerada, sobretudo, na questão da extensão e completude da avaliação da adequação referente a um país. Em outras palavras, trata-se de questionar em que medida a decisão de adequação consegue, de fato, assegurar que todas as transferências em todos os setores cumprem com o nível adequado de proteção de dados pessoais. Com isso em consideração, o WP29 chama atenção para a necessidade de se avaliar se as transferências ou o conjunto de transferência avaliadas na decisão de adequação são de fato representativas de todo país ou de somente um setor ou um estado da federação. Como se vê, o processo de avaliação do terceiro requer uma abordagem transversal a todos os setores do país, visto que a avaliação, quando destinada ao país, será capaz de criar o livre fluxo de dados pessoais sem as salvaguardas

[6] Conforme apontado no WP4, na Europa existe uma tendência histórica de que as regras de proteção de dados estejam previstas em lei, o que garante a possibilidade de sanções serem aplicadas em caso de atividades de tratamento não estarem em conformidade com essas regras, assim como de dar aos indivíduos o direito de reparação. Ainda mais, estas leis preveem mecanismos procedimentais próprios, como o estabelecimento de autoridades supervisoras com poder de monitoramento e funções de investigação. Os mecanismos procedimentais, segundo o WP29, estavam previstos na Diretiva nos temas sobre responsabilidade, sanções, remédios, autoridades supervisoras e notificação. Constata-se, no entanto, que tais mecanismos de conformidade não são tão comuns de encontrar em outras jurisdições.

adicionais e sem as demais hipóteses de exceção aplicáveis a todas as empresas participantes.

Em seguida, convém destacar que o WP29 utilizou o termo *white-list* para se referenciar aos países que são considerados com nível de proteção de dados pessoais adequados. Todavia, caso um país não esteja incluído em tal lista, não se trata necessariamente que este país esteja classificado como um país em que não se tem nível adequado de proteção de dados pessoais, mas tão somente que não há, até o momento, uma avaliação definitiva a respeito do sistema jurídico deste país terceiro. Em relação a criar uma lista sobre os países não recomendados como adequados, no WP4 destaca-se que seria politicamente sensível dispor de uma lista que classificasse os países por meio da lógica inversa, classificando os sistemas jurídicos em que não se garante a proteção adequada.

O WP 29 ainda evidencia certas categorias de transferência que carregam maior potencial de riscos ao titular de dados pessoais, dentre elas, encontram-se aquelas relacionadas a: (i) certos tipos de dados considerados sensíveis pela Diretiva (definido em seu artigo 8º)[7]; (ii) transferências em que se tem riscos de perda financeira (por exemplo, pagamento por cartão de crédito na internet); (iii) transferências em que se carrega riscos relacionados à segurança pessoal do titular de dados; (iv) transferências cuja finalidade é emitir decisões em que afetem significativamente o indivíduo, como, por exemplo, a aprovação de crédito; (v) transferências que podem resultar em ações específicas que constituem intrusão significativa à vida privada do indivíduo, como nos casos de ligação telefônica não solicitada; (vi) transferências repetitivas envolvendo quantidade massiva de dados pessoais, como, por exemplo, aquelas originadas na internet.

Para auxiliar e trazer critérios mais concretos sobre o processo de avaliação dos países, o WP29 procurou desenvolver dois parâmetros de análise para tanto. O primeiro recai sobre o conteúdo das leis de um determinado país e o segundo recai sobre alguns critérios procedimentais, relacionados à efetividade das regras, sendo ambos relacionados ao regime de proteção de dados pessoais do país sob análise.

Abaixo segue tabela sistematizando os dois pontos a serem observados pela decisão de adequação na avaliação do sistema jurídico do país terceiro analisado, sendo os critérios divididos em (i) conteúdo e (ii) procedimental. Interessante constatar que, apesar da Diretiva não dispor a respeito dos critérios de autoridade supervisora do país terceiro avaliado, conforme a redação atual do GDPR, o WP 29, desde 1997, elencou este critério como relevante. Em relação

[7] O art. 8º da Diretiva dispõe: "1. Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e vida sexual. " O número (2) do art. 8º da Diretiva prevê as hipóteses que excepcionam a proibição do (1). Este tema é regulado pelo atual GDPR em seu art. 9º, que dispõe: "(1) É proibido o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa." Em seguida, o ponto (2) traz as hipóteses que excepcionam a regra. (PARLAMENTO EUROPEU, 1995, Art. 8).

ao conteúdo do que é importante assegurar pelas leis de um determinado país, o WP29 aponta como necessário garantir certos princípios. A tabela a seguir sistematiza ambos critérios de análise.

Tabela 7 – Critérios de análise

Conteúdo	**Procedimento/ Enforcement**
- Princípio da finalidade do tratamento; - Princípio da qualidade e proporcionalidade: dados devem ser adequados, relevantes, não excessivos e atualizados para a finalidade pela qual estão sendo transferidos; - Princípio da transparência: os indivíduos devem ser informados sobre as finalidades do tratamento e a identidade dos controladores no país terceiro, e outras informações necessárias; - Princípio da segurança; - Direito de acesso, retificação e oposição; - Restrições a transferência subsequente a países terceiros; Exemplos de princípios adicionais aplicáveis a tipos específicos de tratamento: - Dados sensíveis: salvaguardas adicionais devem ser asseguradas, como requisição de consentimento explícito do titular para o tratamento; - Marketing direto: onde os dados são transferidos para a finalidade de marketing direto, o titular deve ser capaz de realizar o opt-out (retirada) no que toca ao uso de seus dados para estas finalidades; - Decisão automatizada: quando a finalidade da transferência é de obter uma decisão individual automatizada, no sentido do artigo 15 da Diretiva, o indivíduo deve ter o direito de saber a lógica envolvendo esta decisão, e outras medidas devem ser tomadas para resguardar o legítimo interesse do indivíduo.	- Supervisão externa na forma de autoridade independente; - Existência de sanções efetivas e dissuasivas necessárias para assegurar o *enforcement* de regras; - Verificação de conformidade por autoridades, auditores ou oficias independentes de proteção de dados pessoais; - Investigação independente; - Meios apropriados para os titulares que tiveram seus direitos violados: sistema de conciliação independente, que permita a compensação financeira e imposição de sanções.

A respeito do conteúdo, o WP29 já sinalizava que países terceiros deviam prever em seu direito doméstico certos padrões de proteção de dados pessoais. Em primeiro lugar, destaca-se

a necessidade de garantir que o tratamento de dados pessoais seja realizado mediante uma finalidade específica, bem como seu uso subsequente ou sua comunicação deve ocorrer somente se não forem incompatíveis com a finalidade da transferência. A única exceção possível a esta regra seria por meio do que disposto no artigo 13 da Diretiva, como exemplo de questões envolvendo segurança do Estado, defesa, segurança pública, prevenção, investigação, detecção e repressão de infrações penais entre outras hipóteses dispostas expressamente no artigo 13[8]. Em outras palavras, o WP29 estaria delimitando as possibilidades aceitas para que dados pessoais transferidos a terceiros possam ser usados para outra finalidade não inclusa dentro daquela que justificou a transferência. O parâmetro, no entanto, para possíveis exceções é o próprio direito da União Europeia, visto que o WP29 faz referência à própria regra do artigo 13 da Diretiva.

Adicionalmente, o WP 29 ressalta aspectos característicos à qualidade do dado coletado, bem como de sua relevância. Estes dados devem ser exatos e, quando necessários, atualizados. Devem ser adequados, relevantes e não excessivos para o cumprimento das finalidades pelas quais são transferidos ou tratados. Aos indivíduos, deve ser dada informações a respeito da finalidade do tratamento e da identidade do controlador no país terceiro, sendo possível permitir exceções que se encaixem nos artigos 11 (2) e 13 da Diretiva. O artigo 11 (2) versa sobre tratamento com finalidades estatísticas, histórica ou de investigação científica. O artigo 13, por sua vez, versa sobre restrições impostas em caso de segurança do Estado, defesa, de segurança pública, prevenção investigação e repressão de infrações penais e demais hipóteses previstas.

O tratamento dos dados deve respeitar medidas de segurança técnicas e organizacionais. Ao titular de dados deve ser garantido o direito de acesso, retificação e oposição, bem como deve-se ter garantias de que há restrições para a transferência a outros países terceiros, devendo ser permitido a transferência subsequente somente se o país terceiro garanta nível adequado de proteção. Neste último caso, as únicas exceções seriam aquelas contidas no artigo 26 da Diretiva, como nos casos de consentimento, execução de contrato, proteger interesses vitais entre outros.

No que toca aos princípios adicionais a serem aplicados a tipos específicos de tratamento de dados, o documento WP4 ressalta para a necessidade de salvaguardas adicionais em casos de tratamento de dados sensíveis, como o requisito de que o titular dos dados tenha consentido

[8] "Art. 13º Derrogações e restrições 1. Os Estados-membros podem tomar medidas legislativas destinadas a restringir o alcance das obrigações e direitos referidos no nº 1 do artigo 6º, no artigo 10º, no nº 1 do artigo 11º e nos artigos 12º e 21º, sempre que tal restrição constitua uma medida necessária à protecção: a) Da segurança do Estado; b) Da defesa; c) Da segurança pública; d) Da prevenção, investigação, detecção e repressão de infracções penais e de violações da deontologia das profissões regulamentadas; e) De um interesse económico ou financeiro importante de um Estado-membro ou da União Europeia, incluindo nos domínios monetário, orçamental ou fiscal; f) De missões de controlo, de inspecção ou de regulamentação associadas, ainda que ocasionalmente, ao exercício da autoridade pública, nos casos referidos nas alíneas c), d) e e); g) De pessoa em causa ou dos direitos e liberdades de outrem. 2. Sob reserva de garantias jurídicas adequadas, nomeadamente a de que os dados não serão utilizados para tomar medidas ou decisões em relação a pessoas determinadas, os Estados-membros poderão restringir através de uma medida legislativa os direitos referidos no artigo 12º nos casos em que manifestamente não exista qualquer perigo de violação do direito à vida privada da pessoa em causa e os dados forem exclusivamente utilizados para fins de investigação científica ou conservados sob forma de dados pessoais durante um período que não exceda o necessário à finalidade exclusiva de elaborar estatísticas."(PARLAMENTO EUROPEU, 1995, p. 13).

de forma explícita ao tratamento ou, nos casos de marketing, que os dados sejam transferidos tendo oferecido mecanismos de *opt-out* (retirada) a qualquer momento. Quanto à questão de tratamento de decisão automatizada, o documento ressalta a necessidade que ao indivíduo seja dado o direito de saber a lógica envolvida na decisão.

Por fim, algumas considerações adicionais feitas no documento WP4 a respeito da Convenção 108 são importantes para esta dissertação. Dentre eles, destaca-se que a Convenção 108 (i) contempla previsão dos princípios acima elencados, com exceção do princípio da transparência, em que, segundo o WP29, existem dúvidas quanto à necessidade advinda da Convenção de que os controladores providenciem informações de forma ativa nos moldes requeridos pelo arts. 10 e 11 da Diretiva[9,10]; (ii) esta não possuía regras de restrição das transferências a países não signatários; e (iii) não fazia nenhuma requisição quanto à autoridade supervisora.

O WP fez estas observações em 1997, o quadro, no entanto, passou a ser modificado em 2004 quando da aprovação do "Protocolo Adicional à Convenção para a Proteção das Pessoas Relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal, Respeitante às Autoridades de Controlo e Aos Fluxos Transfronteiriços de Dados ("Protocolo")". O Protocolo dispõe em seu artigo 1º acerca da autoridade de controlo e no seu artigo 2º trata a respeito do regramento do fluxo transfronteiriço de dados pessoais.

No que se refere à autoridade de controlo, este trata da necessidade de garantir poderes de investigação e intervenção, assim como da possibilidade de judicializar a questão ou leva-las ao conhecimento de autoridade judiciárias competentes. Também prevê a possibilidade de que as autoridades analisem pedidos apresentados por qualquer indivíduo para proteção de seus direitos e liberdades fundamentais. Ressalta a necessidade de independência funcional da autoridade, a possibilidade de contestação judicial das suas decisões e a cooperação com autoridades estrangeiras.

No que se refere ao fluxo transfronteiriço, o Protocolo dispõe que a transferência só deve

[9] "Art. 10º Informação em caso de recolha de dados junto da pessoa em causa. Os Estados-membros estabelecerão que o responsável pelo tratamento ou o seu representante deve fornecer à pessoa em causa junto da qual recolha dados que lhe digam respeito, pelo menos as seguintes informações, salvo se a pessoa já delas tiver conhecimento: a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante; b) Finalidades do tratamento a que os dados se destinam; c) Outras informações, tais como: - os destinatários ou categorias de destinatários dos dados, - o carácter obrigatório ou facultativo da resposta, bem como as possíveis consequências se não responder, - a existência do direito de acesso aos dados que lhe digam respeito e do direito de os rectificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos." (PARLAMENTO EUROPEU, 1995, Art. 10).

[10] "Art. 11º Informação em caso de dados não recolhidos junto da pessoa em causa 1. Se os dados não tiverem sido recolhidos junto da pessoa em causa, os Estados-membros estabelecerão que o responsável pelo tratamento, ou o seu representante, deve fornecer à pessoa em causa, no momento em que os dados forem registados ou, se estiver prevista a comunicação de dados a terceiros, o mais tardar aquando da primeira comunicação desses dados, pelo menos as seguintes informações, salvo se a referida pessoa já delas tiver conhecimento: a) Identidade do responsável pelo tratamento e, eventualmente, do seu representante; b) Finalidades do tratamento; c) Outras informações, tais como: - as categorias de dados envolvidos, - os destinatários ou categorias de destinatários dos dados, - a existência do direito de acesso aos dados que lhe digam respeito e do direito de os rectificar, desde que sejam necessárias, tendo em conta as circunstâncias específicas da recolha dos dados, para garantir à pessoa em causa um tratamento leal dos mesmos." (PARLAMENTO EUROPEU, 1995, Art. 10).

ocorrer se o Estado ou organização assegurar um nível de proteção adequado para a transferência. Em seguida, exemplifica a autorização da transferência mediante duas grandes possibilidades: (i) caso em que o direito interno permite com fundamento em interesses específicos da pessoa em causa ou interesses legítimos prevalecentes, como aqueles de interesse público e (ii) se o agente responsável pela transferência apresentar garantias julgadas suficientes pelas autoridades competentes, como aquelas provenientes de cláusulas contratuais.

Apesar desta observações, já desde 1997, o WP29 sinaliza no WP4 que os países signatários da Convenção parecem indicar um sistema jurídico adequado nos termos do artigo 25 (1) da Diretiva, desde que (i) o país possua mecanismos institucionais adequados, como autoridade independente com poderes apropriados e (ii) o país seja o destino final da transferência e não um intermediário em que os dados apenas transitam. Como se vê, o critério de adequação de um país depende de uma autoridade independente já mesmo antes do GDPR, suas origens remontam os primeiros anos da Diretiva, por meio de interpretação dada pelo WP29.

Por fim, quanto aos tipos de transferência internacional possíveis dentro da relação entre importador e exportador de dados pessoais, o WP29 exemplifica dois tipos. O primeiro em que se configura uma transferência indireta, ou seja, não há contado com o titular de dados pessoais e a segunda em que se configura uma transferência direta entre titular e controlador. Assim, é possível apontar, ao menos, os três tipos a seguir: (i) comunicação de dados pessoais entre um controlador estabelecido na União Europeia e um outro controlador estabelecido em um país terceiro; (ii) comunicação de dados pessoais entre um controlador estabelecido na União Europeia e um outro operador estabelecido em um país terceiro; e (iii) comunicação entre um titular de dados pessoais na União Europeia e um controlador estabelecido em um país terceiro (por exemplo, via telefone ou internet).

3.1.2 Os critérios materiais e procedimentais de um sistema de autorregulação

O segundo documento, "WP7 - Julgando a autorregulação da indústria: quando a autorregulação faz contribuição significativa ao nível de proteção de dados pessoais de um país terceiro?", busca, da mesma forma que o anterior, trazer critérios objetivos para a análise de um setor cujas regras de proteção de dados pessoais estão elencadas em mecanismos de autorregulação da indústria. Da mesma forma, portanto, a avaliação também deve recair sobre (i) o conteúdo do código de autorregulação e o (ii) procedimento/*enforcement* do código.

No que diz respeito ao conteúdo, trata-se de avaliar se o código protege os princípios elencados no WP4, bem como deve o código proibir o compartilhamento/divulgação dos dados aos controladores não membros da autorregulação e que não disponham de outra proteção considerada adequada. Quanto ao procedimento e *enforcement*, critério cuja preocupação está ligada à efetividade das regras, o documento WP7 ressalta a dificuldade maior de se avaliar um

código de autorregulação porque requer entendimento quanto ao modo e os meios em que se garante aderência às suas regras, bem como a forma como os conflitos de não conformidade são solucionados.

Para conseguir conduzir este modelo de avaliação é necessário que haja definição sobre o que está incluso no conceito de autorregulação. Sobre isto, o WP29 define como código de autorregulação (ou outros instrumentos), para os propósitos do documento, um conjunto de regras determinadas por um setor da indústria ou uma categoria profissional que deve ser considerada quando por uma pluralidade de controladores. Segundo dispõe o WP29, este conceito de autorregulação é amplo e permite abarcar tanto código desenvolvido por uma associação pequena de indústria, com poucos membros, até códigos de ética profissionais aplicáveis a toda categoria profissional, como os de ética médica, cuja força é entendida como "quase-jurídica".

Outra peculiaridade a ser considerada em avaliação de modelos de autorregulação diz respeito ao grau de *enforcement* das regras. Neste contexto, a questão recai menos se a associação ou o órgão responsável pelo código representam todos os controladores e operadores do setor ou somente uma pequena porcentagem dele, mas mais se a associação possui força em temos de impor sanções a seus membros pela não conformidade com o código.

Apesar disso, o documento ressalta alguns pontos que fazem os códigos de um setor de indústria ou profissionais com cobertura mais adequada do que as de pequenas associações. Primeiro, do ponto de vista do consumidor, a indústria mais fragmentada ou caracterizada por associações rivais, cada uma com seu código, pode apresentar um sistema de regras confuso. Nesse sentido, a coexistência de diferentes códigos poderia levar a uma imagem de falta de transparência ao titular de dados pessoais. Segundo, em particular em indústria como marketing direto, em que os dados pessoais são rotineiramente compartilhados entre diferentes empresas do mesmo setor, conflitos podem surgir quando as empresas não estejam sujeitas ao mesmo tipo de código de proteção de dados pessoais. Isto pode resultar em um sistema cuja investigação e reclamação pelo consumidor se torna extremamente difícil.

Por fim, no que toca à avaliação do código de autorregulação sob análise, o WP29 destaca três critérios para condução da avaliação. Trata-se de verificar se há (i) um bom nível de conformidade geral; (ii) suporte e ajuda ao titular de dados pessoais e (iii) reparação adequada, incluindo indenização quando cabível.

Quanto ao ponto sobre bom nível de conformidade geral (i), convém destacar como relevante os casos em que o código prevê sanção punitiva em caso de não conformidade. Esta difere da sanção corretiva cujo foco está em alinhar a conduta do agente, de forma a compatibilizar com as exigências do código. Já a punitiva, trata-se de sanção cujo objetivo é ser um incentivo à conformidade por meio de seus efeitos futuros no comportamento do agente.

Quanto ao ponto sobre suporte e ajuda ao titular de dados pessoais (ii), convém destacar como relevante a necessidade de haver mecanismos institucionais de suporte ao titular de dados

pessoais, de forma a garantir que suas dificuldades e reclamações possam ser endereçadas. Adiciona ainda que este suporte institucional deve ser idealmente imparcial, independente e equipado com os necessários poderes de investigação quanto às reclamações dos titulares de dados pessoais. Segundo o documento, algumas questões importantes ao tema são: (i) o sistema permite investigação de reclamações de titulares de dados pessoais?; (ii) como os titulares de dados pessoais tomam ciência do sistema e das decisões referentes aos seus casos individuais?; (iii) existe algum custo envolvido ao titular de dados pessoais?; (iv) quem coordena a investigação? A entidade tem os poderes necessários para tanto?; (v) quem decide os casos de alegação de violação do código?; (vi) São órgãos ou entidades independentes e imparciais?

O documento conclui trazendo considerações a respeito das características importantes ao órgão fiscalizador. A este respeito, afirma a necessidade de ser um órgão considerado independente em relação ao controlador. Entretanto, somente isto ainda não é suficiente para a garantia da imparcialidade. Idealmente, o órgão julgador deve vir de fora do setor industrial ou profissional em questão. A razão para tanto estaria nos interesses em comum que o árbitro/juiz teria em relação ao controlador que sofre com a alegação de violação do código. Uma alternativa para tanto, está na sugestão do órgão ser composto por números equivalentes de representantes da indústria e dos consumidores, respectivamente.

Quanto ao ponto reparação adequada (iii), trata-se da necessidade de estar disponível ao titular de dados pessoais remédios em caso de violação ao código. Dentre os remédios disponíveis, requer-se meios de correção e deleção dos dados, garantias de que o tratamento incompatível com a finalidade anunciada cesse, bem como garantia de indenização em caso de violação de seus direitos. Aqui incluso não somente danos físicos ou financeiros ao titular, mas também psicológicos e morais.

3.2 O caso dos EUA: do Acordo Safe Harbor à sua invalidação

3.2.1 Das negociações ao Acordo Safe Harbor

Em primeiro lugar, é importante ressaltar que os EUA são apresentados de forma desmembrada da tendência global de regular o tema da proteção de dados pessoais por meio de uma legislação que se aplica a todos os setores da economia de forma uniforme, bem como que se aplica às atividades de tratamento desenvolvidas tanto no setor público e privado. Nesse sentido, os EUA apresentam uma abordagem setorial de legislação de proteção de dados pessoais, o que significa dizer que a regulação é aplicada a determinados temas ou criada de forma específica para o setor ou indústria[11].

[11] "Also, there are still many countries with no data protection laws at all as well as countries (most notably the US) with a limited regime, where public regulation of data processing in the private sector is targeted at certain sensitive industries and further provides for data breach notification obligations in respect of specific categories of personal data only."(MOEREL, 2012, p. 26-27).

Assim, diferentemente do modelo aqui já apresentado da União Europeia, os padrões de tratamento dos dados pessoais a serem seguidos pelas empresas não são impostos diretamente por uma legislação federal única, de forma uniforme, com extensão e aplicabilidade a todos os setores[12]. No âmbito federal, a regulação de proteção de dados pessoais e da privacidade do consumidor ocorre, por exemplo, nos setores de prestação de serviços financeiros[13] e de serviço de saúde[14]. A privacidade e informações de crianças no mundo digital também são reguladas em âmbito federal por meio do *Children's Online Privacy Protection Act 1998* (COPPA), o qual define crianças como menores de 13 anos e estabelece a obrigação de implementar as tecnologias disponíveis para obtenção de consentimento parental prévio autorizando qualquer coleta, uso e/ou divulgação de informações das crianças. A obrigação recai sobre os provedores de websites na internet ou que ofereçam serviços online.

No que se refere ao tema à nível estatal, é dada a possibilidade de os estados criarem legislação própria cuja aplicação dos padrões de proteção de dados está limitada às respectivas jurisdições e podem variar em nível de proteção ao consumidor entre estados. Somente a Califórnia, por exemplo, apresenta mais de 25 leis estaduais de privacidade e segurança de dados[15], incluindo o *Consumer Privacy Act* de 2018 (CCPA), que entrou em vigor a partir de 1º de janeiro de 2020[16]. A CCPA possui aplicação aos negócios que cumprem com os requisitos estabelecidos em lei (como, por exemplo, em caso de receita anual maior de 25 milhões de dólares) e assim devem seguir as regras de restrições a coleta, uso e divulgação de informações pessoais[17].

---

12 "In the United States, the laws protecting data privacy have been widely characterized as "sectoral", a reference to fragmented, cross-governmental, and industry-specific regulation. Unlike in Europe, U.S law does not explicitly protect privacy, but constitutional privacy protections implicitly derive from the First, Third, Fourth, Fifth, and Fourteenth Amendments."(CUNNINGHAM, 2016, p. 422).

13 A proteção de informações pessoais coletadas por Bancos, companhias de seguros e outras empresas do setor de serviços financeiros é regulada, por exemplo, por meio do *Gramm Leach Billey Act*.

14 Setor regulado, por exemplo, pelo *Health Information Portability and Accountability Act* (HIPA) e *Health Information Technology and Economic and Clinical Health Act* (HITECH).

15 Informações disponíveis em <https://www.dlapiperdataprotection.com/index.html?t=law&c=US>

16 "The California Consumer Privacy Act (CCPA), enacted in 2018, creates new consumer rights relating to the access to, deletion of, and sharing of personal information that is collected by businesses. It also requires the Attorney General to solicit broad public participation and adopt regulations to further the CCPA's purposes. The proposed regulations would establish procedures to facilitate consumers' new rights under the CCPA and provide guidance to businesses for how to comply. The Attorney General cannot bring an enforcement action under the CCPA until July 1, 2020."Informação disponível em <http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=>.

17 A aplicação da lei respeita alguns critérios, como o de receita anual, número de consumidores ou dispositivos envolvidos ou quando uma porcentagem de 50% ou mais de receitas anuais advém de venda de dados pessoais. Segundo disposto na CCPA, a lei se aplica aquelas organizações que se enquadrem no conceito da lei de "business". Vejamos: (c) "Business" means: (1) A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers' personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers' personal information, that does business in the State of California, and that satisfies one or more of the following thresholds: (A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185. (B) Alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or

Sobre a complexidade do sistema jurídico de proteção de dados pessoais dos Estados Unidos de acordo com seu modelo de legislação federal e estadual, Cunningham (2016) esclarece[18]:

> A regulação dos Estados Unidos torna-se ainda mais complicada pelas legislações estaduais e locais sobre privacidade de dados. Por exemplo, o *Health Insurance Portability and Accountability Act* não possui efeitos preventivos, deixando aos governos estaduais margem para criar legislação adicional referente a informações médicas e de saúde. Quarenta e sete de cinquenta estados possuem leis de notificação de violação, que geralmente exigem que as organizações divulguem quando elas tenham sido hackeadas se "informações pessoais"de terceiros tenham se tornado vulneráveis pela infiltração - com a Califórnia, estado líder em alterações desse tipo na legislação sobre privacidade, promulgando duas novas leis de privacidade em 2013. (CUNNINGHAM, 2016, p. 423) TRADUÇÃO LIVRE

É neste cenário global que a aprovação pela União Europeia da Diretiva 95/46/CE, que elevou o padrão das exigências para tratamento dos dados pessoais e condicionou o cumprimento de diversos requisitos para autorização da transferência internacional aos países terceiros, causou efeitos extraterritoriais interferindo nas relações comerciais entre empresas localizadas no território europeu e aquelas localizadas fora de sua jurisdição.

Os Estados Unidos, por não cumprir com os requisitos estabelecidos pelo regime europeu para se enquadrar como um país com nível adequado de proteção de dados pessoais[19], iniciou, à época, negociações com autoridades europeias para evitar que as empresas localizadas em seu território deixassem de receber os dados das empresas estabelecidas na União Europeia. Para sanar este quadro, em 2000, a União Europeia e os Estados Unidos assinaram o acordo chamado *Safe Harbor*[20], que passou a ser visto como um instrumento capaz de permitir que

devices. (C) Derives 50 percent or more of its annual revenues from selling consumers' personal information.

18 "The industries constrained by data protection legislation are those that traditionally handle sensitive private data. The laws governing data protection often are narrowly tailored, addressing particular elements of personal information or discrete uses of discrete data. U.S regulation is further complicated by state and local data privacy law. For example, the federal Health Insurance Portability and Accountability Act does not have a pre-emptive effect, leaving state governments room to create further legislation affecting medical and health information. Forty-seven of fifty states have breach notification laws, which generally require organizations divulge when they have been hacked if "personal information" of others was made vulnerable by the infiltration, with California a state leader in these changes in privacy legislation, enacting two new privacy laws in 2013."(CUNNINGHAM, 2016, p. 423).

19 "Even the most foundational questions - the definition of "personal information- remain uncertain. The definition of personal information found in the Fair Credit Reporting Act differs from that found in the Video Privacy Protection Act, which in turn differs from that found in the Gramm-Leach-Bliley Act. The Children's Online Privacy Protection Act and the Prohibition on Release and Use of Certain Personal Information from State Motor Vehicle Records employ circular definitions of personal information: the former states that personal information is "individually identifiable information about an individual;"the latter defines personal information as "information that identifies an individual. Disunity among various privacy laws derives from substantial discord ranging from broad policy questions to granular legal applications. Regulatory uncertainty continues to frustrate entities that deal with personal information, particularly those that are reliant on e-commerce, conduct multinational operations, or both." (CUNNINGHAM, 2016, p. 425).

20 Para mais informações: <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/u.s.-eu-safe-harbor-framework>

controladores pudessem transferir dados pessoais para as empresas localizadas nos Estados Unidos assegurando a conformidade com os padrões exigidos na Diretiva 95/46/CE.

Como é possível notar, o quadro de complexidade do direito interno de sistemas jurídicos diferentes deu origem ao Acordo *Safe Harbor*, celebrado entre União Europeia e Estados Unidos. As negociações entre governo americano e europeu ocorreram ao longo de dois anos, até que em 2000 o acordo foi fechado entre os governos com a promessa de servir como ponte para as diferentes abordagens advindas de cada jurisdição no tema[21]. Como dito, o acordo *Safe Harbor* tinha como objetivo fazer com que as organizações que estavam localizadas nos Estados Unidos que recebessem dados de empresas europeias (e, por conta disso, de muitos cidadãos europeus) passassem a cumprir com as exigências de nível adequado de tratamento de dados pessoais semelhante aos padrões da Diretiva.

O WP29 se posicionou algumas vezes a respeito de temas envolvendo o nível de proteção garantido pelo acordo *Safe Harbor*[22]. Dentre seus posicionamentos, é importante ressaltar as preocupações levantadas no "Parecer 07/99 – sobre o nível de protecção de dados fornecido pelos princípios de porto seguro, publicados em conjunto com as questões mais frequentes (FAQ) e outros documentos conexos, em 15 e 16 de novembro de 1999, pelo Departamento de Comércio dos EUA ("WP27")".

Neste documento, o WP29 levantou certos problemas relacionados ao modo de autocertificação das empresas às regras do acordo. Dentre eles, destacam-se aqueles ligados à aparência de que as empresas, por se autocertificarem, estariam cumprindo com as regras do *Safe Harbor*, porém, a ausência de uma fiscalização efetiva poria objeções à real conformidade. Diante disso, as preocupações recaiam em relação a (i) organizações que se autocertificam mas não cumprem com nenhuma das exigências contidas no acordo; (ii) organizações que depois de um ano de autocertificadas, não apareceriam mais na lista de empresas autocertificadas seja porque não renovaram a autocertificação ou seja porque não estão mais qualificadas para tanto; (iii) organi-

[21] "Given the sectoral regulatory framework in the U.S coupled with private sector self-regulation and popular disfavor of an omnibus privacy law, the U.S Department of Commerce and the European Commission negotiated for two years before agreeing to the Safe Harbor exception in 2000. The compromise sought to bridge the differing approaches in the European Union and the United States, streamline the means for U.S organizations to comply with the Directive, and protect E.U organizations transferring personal data to U.S organizations."(CUNNINGHAM, 2016, p. 441).

[22] WP 15: Parecer 1/99 relativo ao nível de proteção dos dados nos Estado Unidos e às negociações em curso entre Comissão Europeia e o Governo dos Estados Unidos (WORKING PARTY, 1999a); WP 19: Parecer 2/99 sobre a adequação dos "International Safe Harbor Principles" (princípios internacionais de porto seguro) enunciados pelo Departamento de Comércio dos EUA em 19 de abril de 1999 (WORKING PARTY, 1999b); WP 21: Parecer 4/99 sobre as questões mais frequentes a publicar pelo Departamento de Comércio dos EUA no quadro da proposta de princípios de porto seguro (WORKING PARTY, 1999c); WP 23: Documento de trabalho sobre o avanço das negociações entre a Comissão Europeia e o Governo dos Estados Unidos da América relativas aos princípios internacionais de porto seguro (WORKING PARTY, 1999d); WP 27: Parecer 7/99 sobre o nível de proteção de dados fornecido pelos princípios de porto seguro, publicados em conjunto com as questões mais frequentes (FAQ) e outros documentos conexos, em 15 e 16 de novembro de 1999, pelo Departamento de Comércio dos EUA (WORKING PARTY, 1999c); WP 31: Parecer 3/2000 relativo ao diálogo UE/EUA sobre o Acordo de porto seguro (WORKING PARTY, 1999a); WP 32: Parecer 4/2000 relativo ao nível de proteção facultado pelos acordos de porto seguro (WORKING PARTY, 1999b).

zações que depois de autocertificadas são adquiridas por outras empresas que não estavam na lista anteriormente (seja porque não cumpre com os critérios ou porque não deseja aderir aos princípios do acordo).

Estes problemas e outros decorrem do fato de que o Acordo *Safe Harbor* estabelece princípios que são de adesão voluntária pelas empresas, na base de medidas de autocertificação e autoavaliação. Assim, a não ser que uma reclamação ou investigação seja conduzida, qualquer organização que se intitule certificada aos princípios estaria apta para receber os dados de empresas localizadas na União Europeia[23].

Apesar de implementado em 2000, a Comissão Federal do Comércio dos Estados Unidos ("FTC")[24] não conduziu nenhuma ação repressiva referente à conformidade das empresas autocertificadas no Acordo até o ano de 2009. Esta situação contribuiu para que críticas surgissem em relação aos mecanismos de *enforcement* das regras contidas no Acordo. Para além disso, havia o problema de pouca adesão em relação à quantidade de empresas, sendo que de 2000 para 2006 a adesão contava com poucas mais de 1100 empresas autocertificadas[25].

Apesar destes problemas, a Comissão reconheceu o Acordo *Safe Harbor* como instrumento capaz de conferir nível adequado de proteção de dados pessoais aos tratamentos de dados vindos da União Europeia, por meio da Decisão 2000/520. Nesta oportunidade, a Comissão Europeia determinou que caso as organizações deem cumprimento aos princípios do Acordo e às diretrizes contidas no documento Questões Mais Frequentes (FAQ), garante-se o nível adequado nos tratamentos dos dados que saem da Comunidade Europeia para o Estados Unidos[26].

Em relação aos princípios, tratava-se de sete princípios que deviam ser assegurados

[23] "The Safe harbor program was voluntary, self-authorized, and minimally enforced. No government official first inspected and determined whether any given company in fact practiced Safe Harbor principles before awarding certification."(CUNNINGHAM, 2016, p. 443).

[24] "A Section 5 da lei Federal Trade Commission Act considera ilegais as «práticas ou actos desleais ou desonestos praticados no comércio ou que nele se reflectem», 15 U.S.C. § 45(a)(1). A mesma norma confere á FTC poderes para actuar contra tais actos e práticas, 15 U.S.C. § 45(a)(2). A FTC pode, segundo a lei e após audiência formal, emitir uma decisão administrativa para fazer «cessar e proibir» as referidas práticas, 15 U.S.C. § 45(b). Se for do interesse público, a FTC pode também procurar obter do tribunal distrital uma restrição temporária ou uma injunção temporária ou permanente, 15 U.S.C. § 53(b). Caso este tipo de práticas se verifique de forma generalizada, ou tenham já sido objecto de decisões administrativas para as fazer cessar e proibir, a FTC pode promulgar uma norma administrativa proibindo os actos ou práticas em causa, 15 U.S.C. § 57a."Trecho retirado do Anexo III da Decisão 2000/520/CE. Disponível em <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000D0520&from=FR>.

[25] (CUNNINGHAM, 2016, p. 447).

[26] O nível adequado de protecção da transferência de dados a partir da Comunidade Europeia para os Estados Unidos da América (EUA), nos termos da presente decisão, pode conseguir-se se as organizações derem cumprimento aos princípios da «privacidade em porto seguro» relativos à protecção de dados pessoais transferidos de um Estado-Membro para os EUA (a seguir denominados «os princípios») e às directrizes das questões mais frequentes (a seguir designadas «FAQ») que servem de guia no que respeita à aplicação dos princípios estabelecidos pelo Governo dos Estados Unidos em 21 de Julho de 2000. Por outro lado, as organizações devem dar a conhecer publicamente as suas políticas em matéria de protecção da vida privada e ficar abrangidas pelo âmbito da competência da Federal Trade Comission (FTC) que, nos termos do artigo 5º da lei relativa ao comércio federal (Section 5 of the Federal Trade Commission Act), garante a proibição dos actos ou as práticas desleais ou enganosas relativas ao comércio, ou de outros organismos públicos que efectivamente assegurem o respeito dos princípios aplicados em conformidade com as FAQ. (COMISSÃO EUROPEIA, 2000b, p. 1).

publicamente pelas empresas, descritos no Anexo 01 da Decisão 2000/520, são eles: (a) aviso; (b) escolha; (c) retransferência; (d) segurança; (e) integridade; (f) acesso e (g) aplicação. A seguir, é apresentado um breve resumo explicando o contexto de interpretação e aplicação de cada um às empresas que se autocertificaram no Acordo.

a) Aviso: Trata-se do dever de informar os titulares quanto à finalidade do tratamento, a forma de contatar a organização para reclamação ou qualquer outra questão, os tipos de terceiros cujos dados são comunicados e as opções e meios que a organização coloca à disposição dos cidadãos para limitarem o tratamento dos dados. O aviso deve ocorrer de forma prévia, clara e visível;

b) Escolha: Trata-se do dever de oferecer a opção de escolha ao titular a respeito do exercício do direito de *opt-out* (retirada) em relação à divulgação de seus dados a terceiros ou quando utilizados para fins incompatíveis com os que justificaram a coleta inicial. Ademais, também requer que aos dados considerados sensíveis (informações pessoais relativas a condições de saúde ou doenças, origem racial ou étnica, opiniões políticas, crenças religiosas ou filosóficas, pertença a sindicato ou informações relativas à vida sexual da pessoa), deve ser dado ao titular o poder de exercer escolha de forma afirmativa e explícita (conhecido como modelo de *opt-in*) em caso de divulgação da informação a terceiros ou utilizá-la para um fim diferente do que inicialmente motivou a coleta. Como se vê, é possível notar que as organizações autocertificadas deviam oferecer mecanismos de retirada aos titulares que descordem do compartilhamento das informações pessoais ou que estas viessem a ser usadas para finalidades diversas daquelas que justificaram a coleta, enquanto o mecanismo era de *opt-in* para aplicação dessas hipóteses em caso de dados sensíveis. Em termos práticos, isto implica dizer que o regime dos dados sensíveis garante maior controle aos titulares de dados visto requerer uma ação afirmativa do titular autorizando o compartilhamento ou a mudança de finalidade. Enquanto para o tratamento dos dados "triviais" bastava a informação e a implementação de mecanismos fáceis e acessíveis para que este venha a exercer o direito de *opt-out*;

c) Retransferência: Trata-se da necessidade de que para divulgar informação a terceiros, a organização deve aplicar os princípios de aviso e escolha. Adicionalmente, as organizações devem certificar se a outra parte subscreve os princípios do *Safe Harbor*, cumpre as disposições da Diretiva ou outras disposições consideradas adequadas. A relação de transferência deve seguir acordo escrito entre os agentes de tratamento, exigindo a garantia do mesmo nível adequado de proteção. Se a organização cumprir com estes requisitos, não será responsável pelo tratamento da informação transferida, a menos que disposto o contrário em contrato ou a organização tenha conhecimento ou devesse ter conhecimento de que o terceiro não toma as medidas razoáveis necessária para cumprimento dos princípios;

d) Segurança: Trata-se do dever de implementar medidas e precauções razoáveis contra perda, utilização e acesso, revelação, alteração ou destruição não autorizada dos dados;

e) Integridade dos dados: Trata-se do dever de manter os dados exatos, completos e atuais para as finalidades estipuladas;

f) Acesso: Trata-se do dever de oferecer ao cidadão o direito de acesso aos dados pessoais que lhes dizem respeito e que estejam em posse de uma organização. Adicionalmente, as organizações também devem dar a opção de retificação, alteração e eliminação de informações inexatas, salvo se as despesas e encargos para tanto forem desproporcionais em relação aos riscos à vida privada da pessoa, ou quando legítimos direitos de terceiros incorram em riscos de violação;

g) Aplicação: Trata-se do dever de inclusão de mecanismos que garantam o cumprimento dos princípios do Acordo *Safe Harbor*, recursos para os titulares que tenham sido afetados pelo descumprimento dos princípios, bem como consequências para as organizações sempre que os princípios não tenham sido cumpridos. As sanções devem ainda ser rigorosas para garantir o cumprimento por parte das organizações.

Em relação às FAQ, tratava-se de questões voltadas ao esclarecimento de diversos temas relacionados à transferência e à proteção de dados pessoais. Os tópicos passam por temas relacionados ao tratamento de dados sensíveis, exceções de aplicação dos princípios quando em contraposição à liberdade de imprensa, papel de autoridades responsáveis pela proteção dos dados, o processo de autocertificação a ser seguido pelas empresas, necessidade de celebração de contratos para a transferência de dados entre os agentes de tratamento, conformidade das empresas aos princípios, regras de resolução de litígio, entre outros.

Em relação às autoridades competentes para investigar denúncias, tomar medidas contra práticas desleais e enganosas e proceder à reparação dos titulares em casos de violação dos princípios e das FAQ, a Comissão Europeia reconheceu como órgão competente o FTC, de acordo com competências estabelecidas no artigo 5º da lei relativa ao comércio federal (*Section 5 of the Federal Trade Commission*) e o Departamento de Transporte, de acordo com as competências conferidas pelo *Title 49 do United States Code, Section 41712*.

3.2.2 Pontos sensíveis no âmbito do Acordo Safe Harbor

Em 2013, a Comissão Europeia emitiu duas Comunicações ao Parlamento Europeu e ao Conselho a respeito de preocupações levantadas sobre a efetividade da proteção conferida aos dados no âmbito das empresas autocertificadas. As Comunicações são: (i) Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Restabelecer a confiança nos fluxos de dados entre UE e os EUA – COM(2013)846 final e (ii) Comunicação da Comissão ao Parlamento

Europeu e ao Conselho sobre o fundamento do sistema Porto Seguro na perspectiva dos cidadãos da UE e das empresas estabelecidas na UE – COM(2013)847 final.

Segundo consta no documento COM(2013)847 final, algumas autoridades da UE manifestaram preocupações sobre (i) os princípios serem formulados de forma muito genérica; e (ii) o quadro depender fortemente da autocertificação e autorregulação, enfrentando problemas, por exemplo, de declarações falsas de autocertificação ou de incorporação incorreta pelos agentes de tratamento dos princípios estipulados no Safe Harbor. Adicionalmente, as empresas estabelecidas na UE manifestaram preocupações a respeito de distorções de concorrência provocadas por uma aplicação insuficiente dos princípios por parte das empresas autocertificadas nos Estados Unidos. Sobre estes pontos, vejamos[27]:

> Algumas das autoridades da UE responsáveis pela proteção de dados estão cada vez mais preocupadas pelas transferências de dados efetuadas no âmbito do atual sistema «porto seguro». Em alguns Estados-Membros, estas autoridades têm criticado o facto de os princípios serem formulados de forma muito geral, bem como de o quadro depender fortemente da autocertificação e da autorregulação. Várias empresas expressam preocupações da mesma ordem, apontando a existência de distorções de concorrência provocadas por uma aplicação insuficiente do sistema. (COMISSÃO EUROPEIA, 2013b, p. 5)

Conforme apontado na Comunicação, a ausência de uma efetiva fiscalização por parte dos EUA em relação ao cumprimento dos princípios pelas empresas autocertificadas gerava ônus de verificação para as autoridades e empresas europeias. Com isso, a Comissão Europeia ressalta o surgimento de diversas ações no âmbito das autoridades nacionais de proteção de dados questionando a efetividade do Acordo *Safe Harbor*. Dentre elas, é possível ressaltar decisão proferida pelas autoridades alemãs[28], em 29 de abril de 2010, que impunha obrigação às empresas que transferem dados da UE para os EUA de verificação ativa se as empresas americanas respeitavam efetivamente os princípios, recomendando que pelo menos a empresa exportadora devia determinar se a certificação da empresa importadora americana continuava válida.

Ademais, com as revelações de 2013 sobre os programas de vigilância dos EUA, a Comunicação prossegue com mais exemplos relacionados às preocupações que surgiram ao longo de diversas autoridades, demonstrando a possibilidade de fragmentação do Acordo *Safe Harbor*. Vejamos[29]:

> Em 24 de julho de 2013, na sequência das revelações sobre os programas de vigilância dos EUA, as autoridades alemãs responsáveis pela proteção de dados deram mais um passo, expressando a sua preocupação pelo facto de «ser altamente provável que os princípios consubstanciados nas decisões da Comissão não estejam a ser respeitados». Existem casos em que certas autoridades

[27] Comissão Europeia (2013b, p. 5).

[28] Conforme consta no link <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__blob=publicationFile>.

[29] Comissão Europeia (2013b, p. 6).

> responsáveis pela proteção de dados (por exemplo, a autoridade de Bremen) solicitaram a uma empresa que transfere dados pessoais para fornecedores americanos que as informassem do modo como estes fornecedores impedem (se tal for o caso) a Agência Nacional de Segurança de aceder a esses dados. A autoridade irlandesa responsável pela proteção de dados indicou que recebera recentemente duas queixas relativamente ao programa «porto seguro», na sequência das revelações publicadas sobre os programas das Agências de Informações dos EUA, embora se tenha recusado a abrir um inquérito pelo facto de a transferência de dados pessoais para um país terceiro satisfazer os requisitos da legislação irlandesa em matéria de proteção de dados. Na sequência de uma queixa semelhante, a autoridade luxemburguesa responsável pela proteção de dados considerou que, quando da transferência de dados para os EUA, as empresas Microsoft e Skype haviam respeitado a lei luxemburguesa relativa à proteção de dados. No entanto, o Supremo Tribunal irlandês deferiu entretanto um pedido de recurso judicial, no âmbito do qual analisará a inação do Comissário irlandês para a proteção de dados relativamente aos programas de vigilância dos EUA. Uma destas duas queixas foi apresentada por um grupo de estudantes intitulado «Europe versus Facebook» (EVF), que submeteu igualmente uma queixa análoga contra a Yahoo na Alemanha, atualmente a ser examinada pelas autoridades competentes em matéria de proteção de dados. Estas reações divergentes das autoridades responsáveis pela proteção de dados face a revelações sobre os programas de vigilância demonstram o risco real de fragmentação do sistema «porto seguro» e levantam questões quanto à sua implementação efetiva.

As preocupações aumentaram no que toca ao acesso a dados pelas autoridades americanas às empresas autocertificadas. A Comunicação ressalta as preocupações principalmente em relação àquelas empresas que participaram do Programa PRISM, o qual permitiu às autoridades americanas o acesso a dados armazenados e tratados nos EUA[30]. Tal acesso, apesar de poder se valer de fundamentos de finalidade de segurança nacional, interesse público ou execução legal - previstos no Acordo *Safe Harbor* -, devem ocorrer respeitados certos parâmetros, como desde que respeitado a medida necessária para cumprir com estes objetivos[31]:

> A Decisão «porto seguro» prevê, no seu anexo I, que a adesão aos princípios de proteção da vida privada pode ser limitada para observar requisitos de segurança

[30] Trata-se, contudo, de ponto sensível em relação à extensão da vigilância, bem como da relação entre autoridades americanas e empresas provedoras de serviços na Internet. A notícia do The Washington Post esclarece um pouco a respeito do que consiste o PRISM: “We know that PRISM is a system the NSA uses to gain access to the private communications of users of nine popular Internet services. We know that access is governed by Section 702 of the Foreign Intelligence Surveillance Act, which was enacted in 2008. Director of National Intelligence James Clapper tacitly admitted PRISM’s existence in a blog post last Thursday. A classified PowerPoint presentation leaked by Edward Snowden states that PRISM enables "collection directly from the servers"of Microsoft, Yahoo, Google, Facebook and other online companies.” Sobre as alegações das empresas provedoras de serviços da internet, a notícia destaca: “In a Friday post titled "What the ...?"Google CEO Larry Page stated that "any suggestion that Google is disclosing information about our users’ Internet activity on such a scale is completely false."Ainda na notícia, destaca-se: In a weekend follow-up, Google chief architect Yonatan Zunger wrote that "the only way in which Google reveals information about users are when we receive lawful, specific orders about individuals."He said that "it would have been challenging — not impossible, but definitely a major surprise — if something like this could have been done without my ever hearing of it."He said that even if he couldn’t talk about such a program publicly, he would have quit Google rather than participate. "We didn’t fight the Cold War just so we could rebuild the Stasi ourselves,"he concluded”. Notícia disponível em <https://www.washingtonpost.com/news/wonk/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/>.

[31] Comissão Europeia (2013b, p. 18-19).

> nacional, interesse público ou execução legal, de legislação, regulamento governamental ou jurisprudência. Para serem válidas, as limitações e restrições ao exercício dos direitos fundamentais devem ser interpretadas de forma restritiva; devem ser enunciadas numa legislação acessível ao público e necessárias e proporcionadas numa sociedade democrática. Em especial, a Decisão «porto seguro» especifica que essas limitações são permitidas apenas «na medida necessária» para observar requisitos de segurança nacional, interesse público ou execução legal. Embora o tratamento excecional de dados para fins de segurança nacional, interesse público ou execução legal esteja previsto no sistema de «porto seguro», quando este sistema foi adotado não era possível prever o acesso em grande escala por parte dos serviços de informações aos dados transferidos para os Estados Unidos no âmbito de transações comerciais.

No que se refere ao segundo documento - Comunicação da Comissão ao Parlamento Europeu e ao Conselho – Restabelecer a confiança nos fluxos de dados entre UE e os EUA – COM(2013)846 final – este ainda afirma que o PRISM afeta os direitos fundamentais dos cidadãos europeus, como o direito à privacidade e aos dados pessoais. O documento aponta para uma existência de vigilância governamental que pode prejudicar a confiança dos usuários na economia digital, repercutindo de forma negativa no seu crescimento[32] Assim, constata-se que os programas de vigilância e a desigualdade de tratamento dos cidadãos da UE com os cidadãos americanos compromete o nível de proteção conferido pelo Acordo. A Comissão Europeia entende que o acesso posterior pelas autoridades americanas acaba por não abranger a finalidade pela qual os dados foram inicialmente transferidos.

Seguindo ainda a exposição de medidas tomadas por autoridades nacionais, a Comissão Europeia destaca que os comissários responsáveis pela proteção de dados da Alemanha decidiram não emitir novas autorizações de transferência de dados para países que não pertençam à UE, envolvendo aquelas emitidas no âmbito da prestação de serviços de computação em nuvem. Adicionalmente, as autoridades ainda iriam avaliar sobre a possibilidade de suspender a transferência de dados fundamentadas nos princípios do *Safe Harbor*[33]. Em seguida, a Comissão Europeia aponta que essas medidas particulares de autoridades nacionais podem acabar por fragmentar a aplicação do Acordo *Safe Harbor*, esvaziando, em certa medida, os objetivos que levaram a sua celebração.

---

[32] "Os programas norte-americanos de recolha de informações em grande escala, como o PRISM, afetam os direitos fundamentais dos cidadãos europeus e, nomeadamente o direito à privacidade e à proteção dos dados pessoais. Estes programas também indiciam a existência de uma ligação entre a vigilância governamental e o tratamento de dados pelas empresas privadas, nomeadamente pelas empresas de Internet norte-americanas, o que pode, assim, ter impacto económico. O facto de os utilizadores da Internet recearem o tratamento em grande escala dos seus dados pessoais pelas empresas privadas ou a vigilância dos seus dados pelos serviços de informações pode prejudicar a sua confiança na economia digital e ter efeitos negativos no crescimento." (COMISSÃO EUROPEIA, 2013a, p. 3).

[33] Os comissários responsáveis pela proteção dos dados na Alemanha decidiram não emitir novas autorizações de transferência de dados para países que não pertençam à UE (por exemplo, para a utilização de certos serviços em nuvem). Irão ainda analisar se se deve suspender a transferência de dados com base nos princípios «porto seguro». O risco daqui decorrente é que essas medidas, adotadas a nível nacional, possam criar diferenças a nível do âmbito de aplicação do sistema, o que significaria que o «porto seguro» deixaria de ser um mecanismo essencial para a transferência de dados pessoais entre a UE e os EUA. (COMISSÃO EUROPEIA, 2013a, p. 8).

De forma a orientar para o restabelecimento da confiança entre EUA e UE, a Comunicação estabelece diversos pontos para aprimoramento na relação entre o país e o bloco no âmbito das regras estipuladas no Acordo *Safe Harbor*. Ainda, esclarece que a revogação do Acordo afetaria negativamente os interesses das empresas, tanto da UE como dos EUA, que são membros do sistema. Por conta disso, ressalta como melhor medida que o *Safe Harbor* seja reforçado em suas regras.

Por fim, convém destacar dois pontos adicionais importantes para o desenvolvimento desta dissertação. O primeiro ponto em que a Comissão Europeia destaca no COM(2013)846 final a necessidade de que os padrões europeus de proteção de dados sejam promovidos internacionalmente, bem como destaca que as relações entre EUA e UE podem ser usada como oportunidade única para estabelecerem uma norma internacional. Nesse sentido, a Comissão reconhece que uma base sólida de normas com força executória entre EUA-UE constituiria uma base sólida para os fluxos transnacionais de dados de modo geral. Ainda reconhece a necessidade de promoção para adesão à Convenção 108 como medida que contribuiria para normas internacionais de proteção de dados.

O segundo ponto diz respeito à observação feita pela Comissão Europeia de que as divulgações de vigilância pelas autoridades americanas provocaram aceleramento interno na aprovação do então GDPR, visto que este acontecimento contribuiu para a percepção da necessidade de reforma das normas de proteção de dados no âmbito do direito da União Europeia.

3.2.3 O Caso Schrems: Invalidando o Acordo Safe Harbor

Em 2015, o Tribunal de Justiça da União Europeia (TJUE) invalidou o Acordo Safe Harbor, no caso Schrems v. Data Protection Commissioner. O caso foi decidido no dia 6 de outubro de 2015 e teve início devido a uma queixa feita pelo nacional e residente na Áustria M. Schrems ao Comissário de Proteção de Dados da Irlanda (Comissário), em que solicitava a proibição da transferência de seus dados pessoais ocorrida entre o Facebook Ireland e Facebook Inc., este último localizado nos Estados Unidos. Segundo consta na decisão, o usuário do Facebook celebra contrato tanto com o Facebook Ireland quanto com o Facebook Inc., o que autoriza a transmissão, no todo ou em parte, dos dados pessoais de residentes na União Europeia para os Estados Unidos[34].

A questão é submetida ao TJUE devido ao pedido de decisão prejudicial apresentado pelo Supremo Tribunal de Justiça da Irlanda, nos termos do artigo 267 do Tratado sobre o Funcionamento da União Europeia (TFUE), o qual dispõe que o Tribunal é competente nos casos que versem sobre a validade e a interpretação dos atos adotados pelas instituições, órgãos ou

[34] "Todas as pessoas que residam no território da União e pretendam utilizar o Facebook são obrigadas, no momento da sua inscrição, a celebrar um contrato com o Facebook Ireland, filial do Facebook Inc., com sede nos Estados Unidos. Os dados pessoais dos utilizadores do Facebook residentes no território da União são, no todo ou em parte, transferidos para servidores pertencentes à Facebook Inc., situados em território dos Estados Unidos, onde são objeto de tratamento."(TJUE, 2015, p. 15).

organismos da União Europeia[35]. Assim, quando suscitado perante órgão jurisdicional nacional e as decisões não sejam suscetíveis de recursos, esse órgão é obrigado a submeter a questão ao TJUE, tramitação que ocorreu no caso *Schrems v. Data Protection Commissioner*.

Em seu pedido, o M. Schrems alegava que as práticas em vigor nos EUA não asseguravam uma proteção suficiente de seus dados pessoais, uma vez que existia grande e conhecida atividade de vigilância por parte das autoridades públicas norte americanas. O reclamante mencionava as revelações feitas por Edward Snowden[36] em relação às atividades dos serviços de inteligência dos EUA e, em particular, da Agência Nacional de Segurança ANS (*National Security Agency* – NSA).

O Comissário arquivou o pedido por falta de fundamento, mediante a justificativa de que ele não era obrigado a investigar as reclamações de M. Schrems, pois não haveria evidência que os seus dados pessoais foram acessados pela ANS e que as alegações levantadas não poderiam prosperar uma vez que toda questão envolvendo adequação da proteção de dados pelos EUA era determinada de acordo com a Decisão 2000/520/CE, em que ficou entendido pela Comissão Europeia que os EUA, na medida do âmbito de aplicação do *Safe Harbor*, garantem o nível adequado de proteção de dados pessoais.

Insatisfeito com a decisão do Comissário, M. Schrems interpôs recurso noa Supremo Tribunal de Justiça da Irlanda, a qual declarou que a vigilância e interceptação eletrônica dos dados pessoais transferidos da UE para os EUA cumprem com o necessário e indispensável objetivo do interesse público. Porém, as revelações do Edward Snowden demonstraram um excesso por parte da ANS e dos órgãos federais dos EUA. Segundo consta na Decisão do TJUE, oa Supremo Tribunal de Justiça da Irlanda se manifestou no seguinte sentido[37]:

> Ora, o acesso massivo e indiscriminado a dados pessoais é, evidentemente contrário ao princípio da proporcionalidade e aos valores fundamentais protegidos pela Constituição irlandesa. Para as interceções das comunicações eletrônicas

[35] "Art. 267: O Tribunal de Justiça da União Europeia é competente para decidir, a título prejudicial: a) Sobre a interpretação dos Tratados; b) Sobre a validade e a interpretação dos atos adotados pelas instituições, órgãos ou organismos da União. Sempre que uma questão desta natureza seja suscitada perante qualquer órgão jurisdicional de um dos Estados-Membros, esse órgão pode, se considerar que uma decisão sobre essa questão é necessária ao julgamento da causa, pedir ao Tribunal que sobre ela se pronuncie. Sempre que uma questão desta natureza seja suscitada em processo pendente perante um órgão jurisdicional nacional cujas decisões não sejam suscetíveis de recurso judicial previsto no direito interno, esse órgão é obrigado a submeter a questão ao Tribunal. Se uma questão desta natureza for suscitada em processo pendente perante um órgão jurisdicional nacional relativamente a uma pessoa que se encontre detida, o Tribunal pronunciar-se-á com a maior brevidade possível." (TFUE, 2012, Art. 267).

[36] "Public concern about cross-border data flows reached an apex in June 2013 after media outlets publicized the revelations of former US National Security Agency (NSA) analyst Edward Snowden. Snowden alleged that the NSA and other surveil- lance agencies were engaged in massive global online surveillance, undermining the privacy of many individuals in the US and abroad. Brazil, India, Turkey, China, and Germany, among other nations, adopted strategies that restricted rather than enhanced the free flow of information (Maxwell and Wolf, 2012; Chander and Le, 2014). Meanwhile, several EU countries and other states tried to use the Snowden revelations to wrest greater market share from the US Internet giants (Chander and Le, 2014; US ITC, 2013; Kommerskollegium, 2014)." (AARONSON, 2015, p. 3).

[37] TJUE (2015, p. 16).

> serem consideradas conformes a essa Constituição, é necessário apresentar provas de que tais interceções têm caráter seletivo, de que a vigilância de certas pessoas ou de certos grupos de pessoas se justifica objetivamente no interesse da segurança nacional ou do combate à criminalidade, e de que existtem garantias adequadas e verificáveis. Assim, segundo a *High Court* (Supremo Tribunal de Justiça), se o processo principal fosse julgado apenas com base no direito irlandês, haria então que concluir que, atendendo à existência de uma dívida séria sobre a questão de saber se os Estados Unidos da América asseguram um nível de proteção adequado dos dados pessoais, o *Commissioner* devia ter procedido a uma investigação dos factos denunciados por M. Schrems na sua queixa, e que não teve razão ao arquivá-la. (TJUE, 2015, p. 16)

Conforme trecho acima, segundo o próprio Supremo Tribunal de Justiça da Irlanda, se a decisão fosse ser julgada exclusivamente sob a lei da Irlanda, então o Comissário deveria ter procedido com a investigação solicitada pelo M. Schrems. Isto porque o acesso massivo e indiscriminado a dados pessoais é contrário ao que dispõe a própria Constituição irlandesa. Para que tais práticas venham a ser consideradas válidas perante a Constituição irlandesa, é necessário que se apresente provas de que tais interceptações têm caráter seletivo e de que a vigilância de certos grupos e pessoas se fundamenta objetivamente no interesse da segurança nacional ou do combate à criminalidade, assegurando aos titulares disponibilização de garantias adequadas.

Todavia, o Supremo Tribunal de Justiça da Irlanda entendeu que o caso deveria ser julgado à luz do direito da União Europeia, em conformidade com o disposto no artigo 51 da Carta dos Direitos Fundamentais da União Europeia (CDFUE)[38]. Em seguida, o Supremo Tribunal de Justiça observou que apesar do M. Schrems não ter contestado direta e formalmente a validade da Decisão 2000/520, cabe ao TJUE se manifestar acerca da possibilidade do Comissário se afastar do entendimento estabelecido pela Comissão Europeia em decisão de adequação. Assim, questiona-se o TJUE se o responsável pela administração e *enforcement* da proteção de dados está absolutamente vinculado pela Decisão 2000/520 tendo em consideração os artigos 7º, 8º e 47 da (CDFUE) e o artigo 25 (6) da Diretiva 95/46 ou o oficial de dados pode/deve conduzir investigação sobre a matéria à luz dos últimos desenvolvimentos dos fatos?

O TJUE decidiu que: (i) apesar de autoridades nacionais não terem competência para invalidar o ato da União Europeia, a autoridade supervisora de um Estado Membro responsável pela proteção do tratamento de dados não fica impedida de examinar a reclamação de um titular sobre possível violação do país terceiro no que tange às leis e às práticas em vigor no tratamento de seus dados mesmo quando a Comissão Europeia decide que um país terceiro garante proteção adequada aos dados pessoais; e (ii) a Decisão 2000/520 é inválida.

Em relação ao poder de investigação da autoridade, a Corte ressaltou o dispositivo 28

[38] "Art. 51. Âmbito de aplicação 1. As disposições da presente Carta têm por destinatários as instituições e órgãos da União, na observância do princípio da subsidiariedade, bem como os Estados-Membros, apenas quando apliquem o direito da União. Assim sendo, devem respeitar os direitos, observar os princípios e promover a sua aplicação, de acordo com as respectivas competências. 2. A presente Carta não cria quaisquer novas atribuições ou competências para a Comunidade ou para a União, nem modifica as atribuições e competências definidas nos Tratados." (UNIÃO EUROPEIA, 2000, art. 51).

e o Considerando 63 da Diretiva e firmou entendimento que as referidas autoridades gozam de poderes de inquérito, tais como recolher todas as informações necessárias ao desempenho das suas funções de controle. Assim, estão inclusos poderes efetivos de intervenção, tais como proibir temporária ou definitivamente um tratamento de dados ou, ainda, do poder de intervir em processos judiciais. As autoridades possuem prerrogativa, portanto, de verificar se uma determinada transferência de dados pessoais do seu país para um terceiro respeita os requisitos estabelecidos pela Diretiva.

A seguir, o trecho resume o que ficou decidido pelo TJUE no âmbito de apreciação pelas autoridades nacionais no que toca às reclamações dos titulares de dados relativos à transferência internacional de dados pessoais:

> Atendendo às considerações anteriores, há que responder às questões submetidas que o artigo 25., n. 6, da Diretiva 95/46, lido à luz dos artigos 7.º, 8.º e 47.º da Carta, deve ser interpretado no sentido de que uma decisão adotada ao abrigo desta disposição, como a Decisão 2000/520, através da qual a Comissão constata que um país terceiro assegura um nível de proteção adequado, não obsta a que uma autoridade de controle de um Estado-Membro, na aceção do artigo 28. desta diretiva, examine o pedido de uma pessoa relativo à proteção dos seus direitos e liberdades em relação ao tratamento de dados pessoais que lhe dizem respeito que foram transferidos de um Estado-Membro para esse país terceiro, quando essa pessoa alega que o direito e as práticas em vigoe neste último não asseguram um nível de proteção adequado. (TJUE, 2015, p. 21)

Apesar desse poder, enquanto a decisão da Comissão não for declarada inválida pelo TJUE, os Estados-membros e os seus órgãos, que incluem as suas autoridades de supervisão independentes, não podem adotar medidas contrárias a essa decisão, como os atos destinados a determinar que o país terceiro não garante um nível adequado de proteção. Isto porque, em princípio, presume-se que os atos das instituições da UE são válidos e produzem efeitos jurídicos até o momento em que são revogados, anulados ou declarados inválidos. Nesse sentido, pode-se concluir que as autoridades possuem competência para ordenar o término de uma determinada transferência, temporária ou permanentemente, porém não possui competência para decidir, em contrário à Comissão, que o país avaliado não garante nível de proteção adequado.

Com isto exposto, ficou decidido que, apesar desta presunção de legalidade dos atos da Comissão Europeia, a decisão de adequação não pode impedir que os titulares cujos dados pessoais foram ou possam ser transferidos para um país terceiro contestem seus direitos perante as autoridades nacionais. Do mesmo modo, a decisão de adequação não pode suprimir nem reduzir os poderes expressamente concedidos às autoridades nacionais de supervisão conforme constava no artigo 28, da Diretiva e artigo 8º, nº 3, da CDFUE.

Neste sentido, a única forma capaz de invalidar o ato da Comissão Europeia é por meio do TJUE (a decisão cita jurisprudência alinhada nesse sentido), sendo que as autoridades nacionais não possuem competência para que elas próprias invalidem a decisão de adequação.

Em relação à Decisão 2000/520, o TJUE decidiu pela invalidade dos artigos 1º e 3º da Decisão 2000/520 proferida pela Comissão Europeia que reconhecia a adequação das transferências ocorridas entre UE e EUA no âmbito do Acordo *Safe Harbor*. Por conseguinte, a invalidação destes dois artigos, segundo decidido pelo TJUE, afeta a validade da Decisão em sua totalidade. O artigo 1º dispunha sobre a adequação da proteção dos Princípios aplicados em conjunto com as Questões Mais Frequentes (FAQ)[39] e o artigo 3º, por sua vez, estabelecia a possibilidade de suspensão da transferência pelas autoridades nacionais para uma organização que tenha sido autocertificada no Acordo quando verificado a necessidade da proteção nos casos de (i) determinação por autoridade americana ou de mecanismo independente de que a transferência violou os Princípios ou (ii) existirem altas probabilidades de supor que os princípios não estão sendo respeitados[40].

[39] "Art. 1º Nos termos do n. 2 do artigo 25.o da Directiva 95/46/CE, para efeitos de todas as actividades abrangidas pelo âmbito da directiva, considera-se que os "princípios da privacidade em porto seguro"(a seguir denominados "os princípios") que figuram no anexo I da presente decisão, aplicados em conformidade com a orientação que proporcionam as questões mais frequentes (a seguir designadas "FAQ"), publicadas pelo Department of Commerce dos EUA, em 21 de Julho de 2000 que figuram no anexo II da presente decisão, asseguram um nível adequado de protecção dos dados pessoais transferidos a partir da Comunidade Europeia para organizações estabelecidas nos Estados Unidos da América, tendo em conta os seguintes documentos emanados do Department of Commerce dos EUA: a) O resumo global de aplicação dos princípios de porto seguro que figura no anexo III; b) O memorando sobre danos por violação das regras de protecção da vida privada e autorizações explícitas previstas na lei dos EUA, que figura no anexo IV; c) O ofício da Federal Trade Commission que figura no anexo V; d) O ofício do Department of Transportation que figura no anexo VI. 2. No que respeita a cada transferência de dados: a) A organização destinatária dos dados comprometer-se-á clara e publicamente a cumprir os princípios aplicados em conformidade com as FAQ; e b) A referida organização fica sujeita aos poderes legais dos entes públicos administrativos norte-americanos referidos no anexo VII da presente decisão, com competência para investigar denúncias, tomar medidas contra práticas desleais e enganosas, assim como proceder à reparação de pessoas singulares, independentemente do seu país de residência ou da sua nacionalidade, sempre que se verificar incumprimento dos princípios segundo as orientações das FAQ." (COMISSÃO EUROPEIA, 2000b).

[40] "Art. 3º 1. Sem prejuízo da competência para tomar medidas que garantam o cumprimento das disposições nacionais adoptadas por força de outras disposições além das previstas no artigo 25.o da Directiva 95/46/CE, as autoridades competentes dos Estados-Membros podem exercer as suas competências para suspender a transferência de dados para uma organização que tenha declarado a sua adesão aos princípios aplicados em conformidade com as FAQ, se isso se verificar necessário à protecção das pessoas no que diz respeito ao tratamento dos seus dados pessoais, nos casos seguintes: a) A entidade pública administrativa norte-americana referida no anexo VII da presente decisão, ou um mecanismo de recurso independente, nos termos da alínea a) do princípio de aplicação que figura no anexo I da presente decisão, determinou que a organização violou os princípios em conformidade com as FAQ; ou b) Existem fortes probabilidades para supor que os princípios não estão a ser respeitados. Há indícios de que o mecanismo de aplicação em causa não toma ou não tomará as medidas adequadas na altura necessária para resolver o caso em questão, que a continuação da transferência dos dados pode causar graves prejuízos às pessoas em causa e que as entidades competentes nos Estados-Membros envidaram esforços razoáveis, dadas as circunstâncias, para facultar à organização em causa a informação e oportunidade necessárias para responder. A suspensão cessará assim que o respeito dos princípios aplicados em conformidade com as FAQ estiver assegurado e a autoridade competente em questão na Comunidade Europeia seja disso informada. 2. Os Estados-Membros devem informar imediatamente a Comissão da adopção de medidas nos termos do n.1. 3. Os Estados-Membros e a Comissão devem ainda manter-se mutuamente informados relativamente aos casos em que os organismos responsáveis pelo cumprimento dos princípios aplicados em conformidade com as FAQ nos Estados Unidos da América não garantam esse mesmo cumprimento. 4. Se a informação recolhida nos termos dos n. 1 a 3 demonstrar que os organismos responsáveis pelo cumprimento dos princípios em conformidade com as FAQ nos Estados Unidos da América não desempenham eficazmente as suas funções, a Comissão deve informar o Department of Commerce norte-americano e, se necessário, apresentar um projecto de medidas, de acordo com o procedimento estabelecido no artigo 31. da directiva, para revogar ou suspender a presente decisão ou limitar o seu âmbito." (COMISSÃO EUROPEIA, 2000b).

No que se refere ao artigo 1º da Decisão 2000/520, o TJUE considerou que a Comissão violou o dispositivo 25, nº 6 da Diretiva ao não avaliar que os Estados Unidos como um todo asseguram efetivamente o nível adequado de proteção, tendo em consideração a sua legislação interna e os compromissos internacionais assumidos. Adicionalmente, o TJUE pontua que o acesso por autoridades públicas de forma generalizada ao conteúdo de comunicações eletrônicas viola direitos fundamentais e o respeito à vida privada, tal como garantido no artigo 7º da CDFUE.

No que se refere ao artigo 3º da Decisão 2000/520, o TJUE entendeu que este dispositivo priva as autoridades nacionais de desempenharem plenamente os poderes conferidos pela Diretiva em seu artigo 28. O TJUE entendeu, assim, que a Comissão ultrapassou sua competência ao delimitar o âmbito de atuação das autoridades[41]

Diante do exposto, a decisão do TJUE concluiu pela invalidade da Decisão 2000/520, o que, em termos práticos, significa dizer pelo não reconhecimento do nível adequado de proteção às transferências que estavam ocorrendo com base no Acordo *Safe Harbor*. Assim, os Estados Unidos passavam a não contar mais com uma decisão que permitisse o livre fluxo de dados entre Estados Unidos e União Europeia. Como se verá, o quadro é solucionado pela adoção de novo acordo entre o país e o bloco, chamado de *Privacy Shield*.

[41] "O artigo 3º, nº 1, primeiro parágrafo, da Decisão 2000/520 deve, portanto, ser entendido no sentido de que priva as autoridades nacionais de controlo dos poderes que lhes são conferidos pelo artigo 28º da Diretiva 95/46 no caso de uma pessoa apresentar, por ocasião de um pedido nos termos desta disposição, elementos suscetíveis de colocar em causa a compatibilidade com a proteção da vida privada e das liberdades e direitos fundamentais das pessoas de uma decisão da Comissão que tenha constatado, com base no artigo 25º, nº 6, desta diretiva, que um país terceiro assegura um nível de proteção adequado. Ora, o poder de execução atribuído pelo legislador da União à Comissão no artigo 25º, nº 6, da Diretiva 95/46 não confere a esta instituição competência para limitar os poderes das autoridades nacionais de controlo referidos no número anterior do presente acórdão. Nestas condições, há que concluir que, ao adotar o artigo 3º da Decisão 2000/520, a Comissão ultrapassou a competência que lhe é atribuída pelo artigo 25º, nº 6, da Diretiva 95/46, lido à luz da Carta, e que esse artigo é, por essa razão, inválido."(TJUE, 2015, p. 26).

4 A DECISÃO DE ADEQUAÇÃO: COMO A COMISSÃO EUROPEIA DECIDE?

Este capítulo analisa as 13 decisões de adequação proferidas pela Comissão Europeia desde a publicação da Diretiva 95/46/CE. A primeira delas foi em relação à Suíça, proferida no ano de 2000. A decisão da Suíça foi seguida por Canada (2001), Guernsey (2003), Argentina, (2003), Ilha de Man (2004), Jersey (2008), Andorra (2010), Faroe Island (2010), Israel (2011), Nova Zelândia (2012), Uruguai (2012), Estados Unidos no âmbito de proteção do *Privacy Shield* (2016) e, por fim, o Japão (2019).

A divisão das análises dos países a seguir se deu em três blocos distintos. O primeiro analisa a decisão da Suíça, proferida em 2000, até a decisão do Uruguai, proferida em 2012. O segundo analisa a decisão dos Estados Unidos de forma apartada, isto porque a decisão possui particularidades que sobressaem na relação entre UE-EUA no tema, merecendo a abordagem apartada visto a complexidade da relação. Conforme já apontado no capítulo anterior, os EUA, por exemplo, já contavam com uma decisão no âmbito do Acordo *Safe Harbor*, a qual foi invalidada a partir da decisão proferida pelo TJUE no Caso Schrems. A nova decisão de adequação analisa o novo acordo *Privacy Shield* e requer, com isso, uma análise apartada das demais, visto a complexidade já pré-estabelecida entre o país e o bloco. Por último, é analisada a decisão do Japão, a qual representa a primeira decisão de adequação proferida sob a vigência do GDPR.

Ao final de cada decisão, busca-se apontar quais critérios aparecem como relevantes na análise do sistema jurídico, legislação ou Acordo sob avaliação pela Comissão Europeia. Para tanto, são retomados os critérios globais e europeus, conforme estipulado por Greenleaf e já mencionado no Capítulo 01. Ressalta-se, de antemão, que a aparição do critério não significa que este tenha sido explorado pela Comissão Europeia em relação a sua forma de implementação e especificidades quando inserido em um contexto jurídico específico. Ao contrário disto, o levantamento e análise de todas as decisões de adequação demonstraram que a Comissão Europeia pouco aprofundou em sua avaliação no que toca à implementação do princípio ou direito mencionado. Conforme será demonstrado, somente nas decisões proferidas na avaliação dos Estados Unidos e Japão, a Comissão Europeia trata dos padrões de proteção de forma mais específica.

As duas Tabelas a seguir apresentam os padrões globais e europeus mencionados nas decisões de adequação analisadas por países. Convém ressaltar, no entanto, que a ausência de menção não sinaliza pela não observação de tal padrão pelo país, mas tão somente a ausêcia desta observação na decisão de adequação proferida pela Comissão Europeia. Eventual silêncio na decisão pode ser argumentado que venha a ser suprido por meio da observação genérica contida nas decisões de que o país ou legislação em avaliação cumprem com os princípios garantidos na

Diretiva 95/46/CE. Contudo, aqui se argumenta que a sua não menção expressa traz incerteza quanto à referência a quais princípios o país ou legislação terceira em análise garantem.

Tabela 8 – Padrão Global e sua menção nas decisões por países

Padrão Global	Suíça (2000)	Canada (2001)	Guernsey (2003)	Argentina (2003)	Ilha de Man (2004)	Jersey (2008)	Andorra (2010)	Faroe Island (2010)	Israel (2011)	Nova Zelandia (2012)	Uruguai (2012)	EUA (2016)	Japão (2019)
Limites na coleta	X											X	X
Qualidade dos dados				X							X	X	X
Finalidade específica da coleta											X	X	X
Aviso da finalidade e dos direitos no momento da coleta												X	X
Uso limitado, divulgação específica ou compatível												X	X
Segurança												X	X
Transparência											X	X	X
Acesso	X		X	X		X					X	X	X
Correção	X			X							X	X	X
Accountability												X	X

Tabela 9 – Padrão Europeu e sua menção nas decisões por países

Padrão Global	Suíça (2000)	Canada (2001)	Guernsey (2003)	Argentina (2003)	Ilha de Man (2004)	Jersey (2008)	Andorra (2010)	Faroe Island (2010)	Israel (2011)	Nova Zelandia (2012)	Uruguai (2012)	EUA (2016)	Japão (2019)
Autoridade de Proteção de Dados	X	X	X	X	X	X	X	X	X	X	X	X	X
Recursos aos Tribunais	X	X	X	X	X	X	X	X	X	X	X	X	X
Restrição às exportações de dados	X										X	X	X
Minimização de dados para finalidade da coleta, não apenas limitada													X
Tratamento lícito e justo, não só a coleta												X	X
Check-in para tipos específicos de tratamento de dados												X	X
Destruição e Anonimização	X		X								X	X	X
Proteções adicionais para dados sensíveis		X				X						X	X
Limites nas tomadas de decisões automatizadas	X											X	X
Opt-out marketing direto												X	X

4.1 O primeiro bloco de análise: avaliação da Suíça ao Uruguai sob a Diretiva

4.1.1 Suíça - 2000

Conforme disposto na decisão de adequação da Suíça, de 26 de julho de 2000, a Suíça protege como direito constitucional o direito à privacidade e, em especial, os dados contra o seu mau uso. O direito foi garantido, após referendo, por meio de uma alteração da Constituição em

18 de abril de 1999 e cuja entrada em vigor se deu a partir de 1 de janeiro de 2000.

A decisão cita que o Tribunal Federal desenvolveu jurisprudência sobre os princípios gerais aplicáveis às atividades de tratamento de dados pessoais mesmo sob a vigência da Constituição anterior, a qual não dispunha de normas específicas sobre o tema. Em especial os casos versavam sobre a qualidade dos dados pessoais, direito de acesso e o direito de requerer a correção e destruição dos dados. Estes princípios vinculam a Federação e os Cantões.

Apesar da ausência de se tratar o tema por meio de norma expressa constitucional até meados de 2000, a Suíça contava com uma lei de proteção de dados pessoais desde 1992 e cuja entrada em vigor se deu em 1 de julho de 1993. Esta lei também prevê mecanismos como (i) direito de acesso; (ii) notificação a autoridades supervisoras independentes sobre as operações de tratamento e (iii) as transferências de dados para países terceiros são estabelecidas por ordem do Conselho Federal. A legislação se aplica às atividades de tratamento dos órgãos federais e cantonais (quando, neste último caso, as operações não estejam sujeitas às disposições próprias de regulação cantonal de proteção de dados pessoais), bem como àquelas atividades desenvolvidas no âmbito do setor privado.

Segundo disposto na decisão, muitos Cantões adotaram legislações específicas de proteção de dados pessoais em matérias nas quais são considerados competentes para legislar, como nos casos de regras vinculadas a hospitais públicos, ao sistema educacional, tributação e poder de polícia. Independente da fonte normativa das regras adotadas pelos Cantões, a decisão ressalta que todos devem aderir aos princípios constitucionais.

Ademais, ressalta-se que a Suíça aderiu em 1997 à Convenção 108, evidenciando que as Partes devem não somente incorporar os princípios contidos na Convenção, mas também cumprir com os mecanismos de cooperação entre as partes. Nesse sentido, as autoridades suíças devem cooperar com outras autoridades dos países signatários quando em face de solicitação de informação sobre o direito suíço e das práticas administrativas de proteção de dados pessoais, bem como com informações a respeito de qualquer instância de tratamento automatizado de dados pessoais. Ainda devem garantir assistência a titulares de dados fora do país para que possam exercer seus direitos, como o de der informado sobre a existência de tratamento de seus dados pessoais, o direito de acesso ou de solicitar que sejam corrigidos, deletados e que haja remédios judiciais disponíveis para os titulares.

Apesar de os princípios poderem sofrer com limitações para proteger interesses públicos, a Comissão Europeia entendeu que a Suíça garante a proteção a todos os princípios necessários para os parâmetros do nível adequado de proteção. Estes princípios podem ser ainda supervisionados e questionados por meio de supervisão independente, com poderes de intervenção e investigação, bem como por meio de remédios judiciais disponíveis aos titulares de dados pessoais. Em caso de danos ocasionados por meio de tratamento ilícito, a decisão ressalta a possibilidade de se aplicar disposições de responsabilidade civil. Vejamos:

> As normas legais aplicáveis na Suíça englobam todos os princípios de fundo necessários para a constatação de um nível de protecção adequado das pessoas singulares, embora estejam também previstas excepções e limitações para a salvaguarda de interesses públicos importantes. A aplicação dessas normas é garantida pela possibilidade de recursos jurisdicionais e pelo controlo independente exercido pelas entidades competentes, como seja o comissário federal dotado de poderes de investigação e intervenção. Por outro lado, em caso de tratamento ilícito que tenha causado dano, aplicam-se as disposições do direito suíço relativas à responsabilidade civil. (COMISSÃO EUROPEIA, 2000b, p. 2)

No que se refere aos padrões globais e europeu de proteção de dados pessoais, foi possível constatar que a decisão tocou em alguns dos tópicos. No entanto, a abordagem do tema se deu de forma bastante superficial, apenas mencionando certos pontos que envolvem alguns padrões globais e europeus de proteção. No que se refere aos padrões globais, foi possível constatar que a decisão menciona a qualidade dos dados (sem especificar o que se entende por isso), assim como menciona a proteção do direito de acesso e correção. Já no que se refere aos padrões europeus, a Comissão menciona a supervisão independente, sem detalhar expressamente a forma como esta supervisão deveria ocorrer (como se por meio de uma autoridade nacional independente), evidencia a existência de recursos aos tribunais disponíveis aos titulares, bem como regras de controle à exportação dos dados pessoais a países terceiros e direito de destruição dos dados. Por fim, trata de forma muito superficial, apenas mencionando, a necessidade de se garantir informações a respeito de um tratamento automatizado.

A seguir, a tabela sistematiza quais os pontos que aparecerem na decisão relativos aos padrões globais e europeus:

Tabela 10 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Qualidade dos dados - Direito individual de acesso - Direito individual de correção	- Autoridade de proteção de dados independente - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares - Restrição às exportações de dados pessoais para países que não possuem padrão adequado de proteção - Limites em decisões automatizadas e o direito de conhecer a lógica do tratamento automatizado - Direito de destruição

4.1.2 Canada - 2001

A decisão de adequação do Canada está restrita à avaliação da Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA) do Canadá, de 13 de abril de 2000, a qual possui aplicação para as atividades de tratamento desenvolvidas pelos agentes do setor privado, que coletam, usam e divulgam informações pessoais no decorrer das atividades comerciais. Isto implica dizer que a avaliação de nível de proteção não diz respeito a todo o sistema jurídico do Canadá (país terceiro avaliado nos termos da Diretiva), mas recai tão somente na medida em que se aplica o PIPEDA às organizações privadas.

Conforme evidenciado na decisão, a aplicação da Lei canadense se deu de forma gradual e em três estágios distintos, sendo somente no ano de 2004 que sua aplicação passou a valer para todas as organizações que coletem, usem ou divulguem dados pessoais em atividades comercias, independente se a organização é regulada a nível federal ou não.

A decisão destacou os dois estágios que antecederam a sua completa aplicação às atividades de tratamento realizadas com cunho comercial. Em um primeiro momento, a aplicação do PIPEDA se dava somente para as atividades e negócios desenvolvidos a nível federal, excetuando ainda assim os dados de saúde. Nesse estágio, estavam incluídos setores como o aéreo, bancário, de radiodifusão e transporte interprovincial. Também se aplicaria àquelas organizações que divulgassem dados pessoais para outra província ou para fora do Canadá, bem como em relação a dados de empregados de instalações, obras ou empresas de atividades a nível federal (este estágio que durou da aprovação até 1 de janeiro de 2002). Em 2002, a Lei passava a ser aplicada aos dados de saúde e às demais entidades cobertas pela fase anterior. Em seu último estágio, a Lei passaria a cobrir todas as atividades econômicas do setor privado, independentemente do nível federal em que suas atividades fossem desenvolvidas.

Nesse sentido, a decisão ainda destaca que o PIPEDA não se aplica ao setor público regulado à nível provincial e em âmbito federal, este último sujeito ao Federal Privacy Act. Também não estão abrangidas aquelas atividades sem fins lucrativos e atividades de caridade, salvo se tiverem natureza comercial. Os dados de empregados que não tenham aplicação para fins comerciais também estão excluídos, sendo exceção os dados de empregados do setor privado regulado a nível federal[1].

A Decisão cita que o Canadá aderiu as Diretrizes de 1980 da OCDE e esteve entre os países que deu suporte às Diretrizes sobre Arquivos de Dados Pessoais Computadorizados, adotado pela Assembleia Geral das Nações Unidas em 14 de dezembro de 1990. Em seguida, a

[1] "A partir de 1 de Janeiro de 2004, a lei canadiana abrangerá todas as organizações que recolhem, utilizam e divulgam informação pessoal no exercício das suas actividades comerciais, quer a organização seja regulamentada a nível federal ou não. A lei canadiana não se aplica a organizações abrangidas pela lei federal sobre protecção da vida privada (Federal Privacy Act) ou reguladas pelo sector público à escala da província, nem a organizações de carácter não lucrativo e a actividades caritativas, a não ser que sejam de natureza comercial. Da mesma forma, não se aplica a dados sobre o emprego utilizados para fins não comerciais, com excepção dos dados relacionados com os empregados do sector privado regulado a nível federal. O Federal Privacy Commissioner do Canadá pode facultar mais informações sobre estes casos."(COMISSÃO EUROPEIA, 2001, p. 2).

decisão reconhece que o PIPEDA cobre todos os princípios necessários para um nível adequado de proteção, mesmo em caso de salvaguardar interesses públicos e para resguardar em domínio público um certo tipo de informação. A decisão ressalta a previsão de recursos judiciais disponíveis aos titulares, bem como a presença de uma supervisão independente, a cargo de autoridades como o *Federal Privacy Commissioner*, sendo uma entidade federal competente para investigar e intervir.

Por fim, cabe ressalta que a decisão reconhece de forma genérica que os princípios do PIPEDA garantem uma proteção adequada. Ressalta-se, contudo, que a Comissão não justifica ou fundamenta esta afirmação.

Como é possível notar, a decisão não se aprofundou nos parâmetros de proteção, restringindo-se a uma análise de extensão de cobertura e aplicabilidade da lei. Do pouquíssimo que foi abordado em relação aos parâmetros, podemos destacar o tema de uma supervisão independente (apesar de nada dispor a respeito da forma como de fato esta autoridade estaria estruturada), bem como da disponibilização aos titulares de recursos judiciais. Estes dois referentes a padrões europeus de dados pessoais. Sobre os padrões globais, o Canadá é membro da OCDE e aderiu às Diretrizes de 1980 (o que faz presumir pelo cumprimento com os padrões globais).

Tabela 11 – Padrões de proteção

Padrão Global	**Padrão Europeu**
Não foi abordado expressamente, porém ressalta-se que aderiu às Diretrizes de 1980 da OCDE	- Autoridade de proteção de dados independente - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares

4.1.3 Guernsey - 2003

A decisão de adequação do Bailados de Guernsey é de 21 de novembro de 2003. Segundo consta na decisão, Guernsey é um território com completa independência, exceto nos casos relacionados às relações internacionais e de defesa, que estão sob responsabilidade do Governo do Reino Unido. Por conta desses fatores, a Comissão Europeia considera o território como país terceiro frente aos critérios contidos na Diretiva e destaca que a ratificação pelo Reino Unido da Convenção 108 estendeu seus efeitos ao território.

A decisão ainda cita que na lei de proteção de dados de Guernsey, aprovada em 2001 e em vigor desde 1 de agosto de 2002, encontram-se os parâmetros de proteção de dados pessoais que foram baseados na Diretiva 95/46/CE. A decisão esclarece que também há dezesseis instrumentos regulamentares que estabelecem regras específicas de proteção de dados pessoais, os quais complementam a lei em matéria de direito de acesso, tratamento de dados sensíveis, notificação à autoridade de proteção de dados pessoais.

A decisão reconhece que os padrões legais de Guernsey cobrem todos os princípios básicos necessários para um nível adequado de proteção. Estes padrões são garantidos por remédios judiciais e por uma autoridade de supervisão independente, investida do poder de investigação e intervenção, sendo representado na figura do Comissário para proteção de dados.

Como se vê, a decisão não passou por pontos importantes de análise e avaliação do país, bastou-se em afirmar que as normas jurídicas aplicáveis em Guernsey englobam os princípios necessários para um nível de proteção adequado e que estes foram baseados na Diretiva. Outro fator de indicação de adequação é que o país é signatário da Convenção 108 (visto a extensão dos compromissos assumidos pelo Reino Unido ao território).

Contudo, a decisão é silente no momento da descrição de quais e como estes princípios seriam de fato garantidos. A decisão somente menciona, mas não se aprofunda, em pontos como (i) direito individual de acesso; (ii) regras existentes para tratamento de dados sensíveis; (iii) regras de notificação à autoridade de proteção de dados; (iv) controle independente exercido pelas autoridades, como pelo Comissário de proteção dados, com poderes de investigação e intervenção e (v) disponibilidade de recurso judicial. As formas e especificidades de cada um deste ponto não foram objeto de aprofundamento.

Tabela 12 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Direito individual de acesso; - Como é signatário da Convenção 108 já cumpriria com estes padrões.	- Autoridade de proteção de dados independente; - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares; - Proteções adicionais para categorias específicas de dados sensíveis.

4.1.4 Argentina - 2003

A decisão de adequação da Argentina é de 30 de junho de 2003. Nesta decisão, a Comissão Europeia destaca três instrumentos jurídicos do país que regulam o tema da privacidade e proteção dos dados pessoais, sendo (i) a Constituição da Argentina; (ii) a lei de proteção de dados da argentina (*Personal Data Protection Act nº 25.326*) e (iii) o Decreto nº 1.558/2001, este último responsável por complementar a lei e esclarecer pontos que estão sujeitos a interpretações divergentes.

Em relação à Constituição da Argentina, esta possui previsão legal do remédio de *habeas data*. A partir desse remédio, garante-se no sistema jurídico argentino que qualquer pessoa tenha o direito de conhecer o conteúdo e a finalidade dos seus dados pessoais contidos tanto em bancos ou registros públicos como bancos privados. Segundo disposto pela Comissão Europeia, em

caso de falsidade da informação ou seu uso para fins discriminatórios, a pessoa será capaz de demandar a deleção, correção, confidencialidade ou atualização dos dados por meio da garantia deste remédio constitucional. Estes direitos, no entanto, não se aplicam em caso de segredo de fontes jornalísticas. A decisão ainda destaca que a jurisprudência argentina reconheceu o direito ao *habeas data* como fundamental e com norma de aplicabilidade direta.

A lei geral de proteção de dados da Argentina aprofunda o texto constitucional, contendo dispositivos acerca dos princípios gerais de proteção de dados pessoais, os direitos dos titulares de dados, as obrigações dos agentes de tratamento, a autoridade supervisora ou órgão controlador, sanções aplicáveis e regras de processo relativas à reparação judicial e aplicação do *habeas data*. A decisão ressalta que os dispositivos da lei podem ter aplicação a nível federal ou a nível provincial, sendo que esta última também possui competência para elaborar dispositivos específicos sobre o tema.

A decisão também ressalta que as regras de proteção de dados pessoais podem ser reguladas de forma específica relacionada a um setor, como ocorre nos casos de transações de cartão de crédito, estatística, bancário e saúde.

Com estas considerações, a Comissão entendeu que o direito na Argentina cobre todos os princípios necessários para um nível adequado de proteção, mesmo com a possibilidade de exceções e limites em casos de interesses públicos. Concluindo, portanto, que os padrões na Argentina protegem os dados pessoais, sendo considerado relevante para este entendimento os seguintes fatores: (i) o *habeas data* é visto como um remédio judicial especial, simplificado e rápido; (ii) a lei de dados da Argentina prevê uma autoridade de controle, responsável por tomar as medidas necessárias para a conformidade das atividades de tratamento com os objetivos e dispositivos da lei, com poderes de investigação e intervenção; (iii) a Argentina possui sanções penais e administrativas que garantem efeitos dissuasivos; e (iv) os dispositivos que tratam de responsabilidade civil (contratual e extracontratual) se aplicam a qualquer atividade de tratamento ilegal que seja prejudicial a pessoa em questão.

Tabela 13 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Qualidade dos dados, os quais devem ser relevantes, precisos e atualizados - Direito individual de acesso; - Direito individual de correção	- Autoridade de proteção de dados (sem esclarecer quanto ao critério de independência) - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares - Deleção

4.1.5 Ilha de Man – 2004

À similaridade do reconhecimento de Guernsey como país terceiro, a Comissão Europeia decidiu ser a Ilha de Man também uma dependência da Coroa Britânica, que goza de independência, exceto nos casos relacionados às relações internacionais e de defesa, as quais são de responsabilidade do governo do Reino Unido. Diante disso, a ratificação pelo Reino Unido da Convenção 108 estendeu seus efeitos ao território.

Em 2002, a Ilha do Man adotou lei de dados pessoais cuja entrada em vigor estava prevista para o ano seguinte (2003). Esta lei revogou a antiga lei de 1986 sobre o tema. Outras leis responsáveis por regular o tema no país também são citadas, como (i) a Lei de Direitos Humanos, aprovada pelo parlamento em 16 de janeiro de 2001 (não completamente em vigor na época da decisão) e (ii) a Lei de Acesso aos Relatórios e Registros de Saúde, de 1993 (do inglês *Access to Health Records and Reports Act 1993*).

A Comissão considera que o país cobre todos os princípios necessários para garantir o nível adequado de proteção, ressaltando que existem remédios judiciais que garantem a aplicação dos princípios, bem como supervisão independente dirigida por autoridades, com poderes de investigação e intervenção. Contudo, assim como já apontado em outras decisões, a decisão não explorou o conteúdo dos princípios, nem como a forma necessária para a independência da supervisão.

Tabela 14 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Não se aplica	- Autoridade de proteção de dados independente; - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares.

4.1.6 Jersey – 2008

À similaridade do reconhecimento dado à Guernsey e à Ilha de Man, a Comissão Europeia considera Jersey como sendo uma dependência da Coroa Britânica, que goza de independência, exceto nos casos relacionados às relações internacionais e de defesa, as quais são de responsabilidade do governo do Reino Unido. Nesse sentido, a Comissão aponta que, com efeito desde 1957 e 1987, respectivamente, a ratificação pelo Reino Unido da Convenção Europeia de Direitos Humanos (CEDH) e da Convenção 108 foram estendidos ao território.

Em relação ao direito interno de Jersey, a decisão cita a lei de proteção de dados de Jersey, cuja entrada em vigor ocorreu em 11 de novembro de 1987, e duas leis complementares (i) o *Data Protection (Amendment) (Jersey) Law 2005* e (ii) *Data Protection (Jersey) Law 2005 (Appointed Day) Act 2005*. Segundo apontado na decisão, as leis em vigor em Jersey possuem

normas baseadas na Diretiva 95/46/CE. Ainda ressalta-se cumprimento de padrões de proteção como (i) direito de acesso; (ii) proteção adicional para tratamento de dados sensíveis e (iii) notificação à autoridade (nada em específico foi desenvolvido sobre este tópico).

Contudo, como nas demais decisões avaliadas, é possível apontar a ausência de aprofundamento dada aos tópicos em geral. Diante disso, a Comissão conclui de forma genérica que os padrões internos de Jersey cumprem com aqueles dispostos na Diretiva, sem, todavia, explicitar como e quais princípios e direitos são previstos e implementados.

Tabela 15 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Direito individual de acesso.	- Autoridade de proteção de dados independente; - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares; - Proteções adicionais para categorias específicas de dados sensíveis.

4.1.7 Andorra – 2010

Conforme aponta a Comissão Europeia na decisão de adequação de Andorra, o país é um Estado com sistema Parlamentar Co-Principado, com o Presidente da República Francesa e o Arcebispo de Urgel sendo considerados co-príncipes no país.

No que toca a proteção do direito à privacidade, este é assegurado no artigo 14 da Constituição do Principado de Andorra, aprovada por referendo popular em 14 de março de 1993. A lei de proteção de dados de Andorra é datada de 2003 (Lei nº 12/2003 ou *Lei qualificada de protección de dades personales* – LQPDP). A legislação é complementada pelo Decreto Registro Público para Inscrição de Arquivos de Dados Pessoais, de 1 de julho de 2004, e pelo Decreto aprovando as regulamentações da Agência de Proteção de Dados Pessoais de Andorra, de 09 de junho de 2010.

Andorra ratificou a Convenção 108 e seu Protocolo Adicional, assim como a Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950, do Conselho da Europa, em vigor em Andorra desde 22 de janeiro de 1996, assim como o Pacto Internacional de Direitos Civis e Políticos das Nações Unidas, aprovado em 1996 e em vigor em Andorra desde 2006.

A decisão reconhece que os padrões legais de Andorra cobrem todos os princípios básicos necessários para um nível adequado de proteção, apesar de haver limitações e exceções em casos de salvaguardas de interesses públicos. Estes padrões são garantidos por remédios administrativos e judiciais e por uma autoridade de supervisão independente, investida do poder

de investigação e intervenção, conhecida como Agência de Proteção de Dados de Andorra.

Como se vê, assim como nas demais decisões, a Comissão Europeia adotou a afirmação padrão de que o país cobre os princípios de forma a garantir proteção adequada sem, contudo, mencionar a quais princípios de fato a decisão fazia referência em sua análise, bem como sem percorrer pelos detalhes de sua aplicação. Fator relevante para esta decisão foram os compromissos assumidos pelo país, dentre eles, a Convenção 108.

Tabela 16 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Não se aplica	- Autoridade de proteção de dados independente - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares

4.1.8 Ilhas Faroé – 2010

Trata-se de uma comunidade autônoma dentro do Reino da Dinamarca. Quando a Dinamarca se juntou à União Europeia, em 1973, Ilhas Faroé não seguiu o mesmo caminho. Por conta disso, a comunidade foi considerada pela Comissão Europeia como sendo um país terceiro.

A Comissão ressalta que a decisão de adequação abrange somente os agentes receptores de dados que estão submetidos a lei de proteção de dados faroense (*Act n. 17*, de 8 de maio de 2001). A lei não se aplica às atividades de tratamento de dados pessoais desenvolvidas pelas autoridades do Reino da Dinamarca, a decisão aponta as seguintes autoridades: (i) Alto Comissário para as Ilhas Faroé (*the High Commissioner of the Faroe Island*); (ii) o Tribunal das Ilhas Faroé (*the Court of the Faroe Island*); (iii) o Comissário das Ilhas Faroé (*the Commissioner of the Faroe Island*); (iv) os Serviços Prisionais e de Liberdade Condicional das Ilhas Faroé (*the Prison and the Probation Service of the Faroe Island*); (v) o Comando das Ilhas Faroé (*the Island Command Faroes*) e (vi) Médico-Chefe das Ilhas Faroé (*the Chief Medical Officer of the Faroe Island*).

Segundo consta na decisão, a lei de proteção de dados de Ilhas Faroé cumpre com os padrões dispostos na Diretiva, cobrindo todos os princípios básicos necessários para um nível de proteção adequado. Ademais, a aplicação da lei é garantida por remédios judiciais e por supervisão independente pelo Comissário de proteção de dados, investido de poderes de investigação e intervenção.

Tabela 17 – Padrões de proteção

Padrão Global	**Padrão Europeu**

- Não se aplica	- Autoridade de proteção de dados independente - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares

4.1.9 Israel – 2011

O sistema jurídico em Israel não é fundamentado em uma constituição escrita, contudo, conforme aponta a decisão de adequação, o Supremo Tribunal do Estado de Israel conferiu status constitucional a certas "Leis Fundamentais". Segundo esclarece a decisão, o direito ao respeito à vida privada está previsto no artigo 7º da "Lei Fundamental: Dignidade Humana e Liberdades". Este conjunto de Leis Fundamentais são complementadas por diversos outros casos (jurisprudência) decididos pelo judiciário israelense. A Comissão Europeia destaca a relevância destas decisões visto estar o sistema jurídico de Israel fundamentado no *common law*.

Apesar do sistema de *common law*, Israel possui legislação tratando sobre regras que se aplicam a atividades de tratamento de dados pessoais e que buscam garantir a sua proteção (como a Lei nº 5.741/1981). A Lei de dados de Israel foi emendada por último em 2007, de forma a estabelecer novos requisitos para o tratamento de dados pessoais e detalhar a forma de organização da autoridade supervisora do país. Conforme reforçado pela decisão, as normas jurídicas de proteção de dados de Israel se baseiam em grande medida nos padrões da Diretiva 95/46/CE. Apesar desta afirmação, a Comissão não apontou de forma expressa quais são estes padrões reproduzidos dentro do sistema jurídico israelense.

A legislação de proteção de dados é complementada por decisões governamentais que tratam sobre a implementação da Lei, bem como sobre a forma de organização e funcionamento da autoridade supervisora. Outros numerosos instrumentos de proteção de dados pessoais possuem regras específicas aplicadas a setores como financeiro, saúde e registros públicos.

A decisão conferida para Israel está limitada ao tratamento em base de dados automatizadas, visto que o Capítulo 2 da Lei nº 5.741/1981 não se aplica ao tratamento manual de dados pessoais. Diante disso, a Comissão ressalta que a decisão de adequação diz respeito àquelas transferências internacionais que ocorrem em meios automatizados. Assim, em outras palavras, não estão cobertas as transferências que ocorram em meios não automatizados.

Outro fator importante diz respeito ao próprio reconhecimento por parte da Comissão Europeia em relação ao Estado de Israel, o qual passa a ser reconhecido nos limites definido em conformidade com o direito internacional. Diante dessa definição, a Comissão estabelece que as transferências que não estejam cobertas pelo conceito dado ao Estado de Israel pelo direito internacional não estão cobertas pela decisão. Vejamos:

> Os resultados da adequação pertinentes para a presente decisão dizem respeito

> ao Estado de Israel, definido em conformidade com o direito internacional. Outras transferências ulteriores para um destinatário fora do Estado de Israel, definido em conformidade com o direito internacional, devem ser consideradas transferência de dados pessoais para um país terceiro. (COMISSÃO EUROPEIA, 2001, p. 2)

Por fim, convém destacar aqui que a Comissão Europeia afirma que (i) o Estado de Israel cobre todos os princípios básicos necessários ao nível de proteção adequado em relação ao tratamento de bases de dados automatizadas; (ii) garante-se recursos administrativos e judiciais aos titulares de dados pessoais; (iii) existe supervisão realizada por autoridade independente, denominada de Autoridade Israelita para Assuntos Jurídicos, Informação e Tecnologia (ILITA), dotada de poderes de investigação e intervenção.

Tabela 18 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Não se aplica	- Autoridade de proteção de dados independente - Recursos aos tribunais para fins de enforcement dos direitos dos titulares

4.1.10 Nova Zelândia – 2012

Conforme explica a decisão de adequação, a Nova Zelândia é uma ex-colônia britânica que se tornou um domínio independente em 1907, mas somente em 1947 rompeu formalmente seus laços constitucionais com a Grã-Bretanha. Trata-se de um Estado unitário que não possui constituição escrita. A Comissão ainda continua explicando que se trata de um país formado por uma monarquia constitucional e um parlamentarismo democrático, no modelo de Westminster, sendo a rainha da Nova Zelândia Chefe de Estado. A decisão ainda esclarece que no sistema jurídico da Nova Zelândia existem leis com importância constitucional referenciadas como lei maior (*higher law*). O sentido dado a essas leis é de que servem como suporte e fundamento orientando/informando práticas do governo e a aprovação de novas leis. Para além disso, as normas cujo status é de lei maior somente podem ser modificadas mediante consenso entre as forças políticas[2].

A Comissão aponta algumas destas leis que possuem relevância para a proteção de dados pessoais, como: (i) Lei da Carta dos Direitos dos Cidadão (*the Bill of Rights Act*), de 28 de agosto de 1990 (Lei nº 109/1990); (ii) a Lei dos Direitos dos Homen (*the Human Rights Act*), de 10 de agosto de 1993 (Lei nº 82/1993); e (iii) Lei sobre a proteção da vida privada (*the Privacy Act*), de 17 de maio de 1993 (Lei nº 28/1993). O status constitucional dessas leis deriva do fato que no processo de criação e aprovação de novas leis, estas devem ser tomadas em consideração.

[2] A decisão não se aprofunda em detalhes a respeito de qual o procedimento interno para que se tenha consenso na modificação das leis com status constitucionais.

Como se vê, a lei de proteção de dados da Nova Zelândia é anterior à Diretiva 95/46/CE, pois é datada de 1993 (*the Privacy Act*). Apesar de sua anterioridade, a lei da Nova Zelândia não é limitada ao tratamento automatizado de dados (mas se aplica a todos os tipos de tratamento de dados) e sua aplicação recai sobre os setores privado e público, com poucas exceções de aplicação relacionadas a questões de interesse público que se justificam em uma sociedade democrática, segundo apontado pela Comissão Europeia.

Existem vários outros instrumentos regulatórios que também trazem dispositivos protegendo a privacidade e regras para viabilizar reclamações jurisdicionais. Conforme consta na decisão, alguns padrões advêm de legislação enquanto outros dependem de autorregulação setorial, incluindo regulação da mídia (meios de comunicação social), marketing direto, mensagens eletrônicas não solicitadas, pesquisa de mercado, saúde e invalidez, banco, seguros e poupanças. Apesar de citar a diferença da origem dos padrões, em momento algum a decisão expressamente cita os padrões e a forma como se é operacionalizada a autorregulação setorial, ficando silente na diferenciação de que tipo de padrão advém da legislação e que tipo de padrão advém de sistema de autorregulação. No caso de marketing direto, por exemplo, não esclarece qual o padrão adotado pelo país (se *opt-in* ou *opt-out*). Diante disso, destaca-se aqui que a Comissão Europeia pouco se aprofunda na metodologia então estipulada pelo WP29 de análise de sistemas diferentes (apresentada no Capítulo3). A decisão somente menciona de forma descritiva que existe segmentação da origem dos padrões.

Por ser um país de sistema jurídico de *common law*, a decisão também ressalta que dentre os princípios fundamentais do *common law* encontra-se a dignidade do indivíduo. Trata-se de um princípio que orienta as decisões judiciais de forma geral. Com isto em vista, a Comissão destaca que a jurisprudência da Nova Zelândia também já se posicionou em casos envolvendo diretamente aspectos da privacidade, incluindo invasão da privacidade, violação da confiança e proteção acessória em contexto de difamação, perturbação do uso e gozo de bens imóveis, assédio, declarações falsas proferidas de forma dolosa, negligência e outros temas relacionados. Apesar do cuidado em ressaltar temáticas que passaram a compor a jurisprudência da Nova Zelândia, a decisão não faz a ligação entre os tópicos elencados e o tema da proteção de dados pessoais, assim como não esclarece de que forma estas decisões contribuem para que se atinja o nível adequado de proteção de dados pessoais no país.

A Comissão ressalta, assim como nas demais, que a Nova Zelândia garante remédios administrativos e judiciais e uma supervisão independente, por meio do Comissário de Privacidade, que tem os poderes conferidos nos moldes do artigo 28 da Diretiva 95/46/CE e age de forma independente. Ademais, destaca-se que a qualquer parte interessada é garantida a possibilidade de buscar compensação judicial pelos danos sofridos como resultado de tratamento ilegal de dados pessoais.

Conforme se vê, a decisão reconhece que a autoridade da Nova Zelândia possui poderes similares àqueles conferidos pelo artigo 28 da então Diretiva 95/46/CE. Este artigo estabelece

parâmetros e competências conferidos às autoridades nacionais dos países da União Europeia, que inclui critérios como controle independente e, mais especificamente, poderes de inquérito e de intervenção (como exemplo, poderes de ordenar bloqueio, apagamento ou destruição dos dados, proibir temporária ou definitivamente o tratamento, dirigir advertência ou uma censura ao responsável, remeter questão ao parlamento ou outra instituição política e intervir em processo judicial).

Tabela 19 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Não se aplica	- Autoridade de proteção de dados independente - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares

4.1.11 Uruguai – 2012

Conforme aponta a decisão de adequação do Uruguai, este não possui proteção expressa do direito à privacidade e de proteção dos dados pessoais no texto da Constituição do Uruguai de 1967. Todavia, os direitos fundamentais expressos na Constituição não são considerados taxativos, o artigo 72 da Constituição do Uruguai fornece uma lista de direitos, obrigações e garantias que não excluem outros inerentes à personalidade humana ou que derivem da forma republicana de governo.

Nesse sentido, a Lei nº 18.331/2008, que versa sobre a proteção dos dados pessoais e sobre o remédio de *habeas data* do Uruguai (*Ley n. 18.331 de Protección de Datos Personales y Acción de "Habeas Data"*), estabelece que o direito de proteção dos dados pessoais é inerente ao ser humano e assim está incluído no artigo 72 da Constituição. O artigo 332 da Constituição do Uruguai, por sua vez, estabelece que a aplicação desses direitos não deve sofrer barreiras devido à ausência de regulamentação específica sobre o tema, o que significa dizer, portanto, que são direitos dotados de aplicabilidade direta.

A lei de proteção de dados do Uruguai é complementada pelo Decreto nº. 414/2009, de 31 de agosto de 2009, cujo objetivo é esclarecer diversos pontos da lei e estabelecer a organização, poderes e funcionamento da autoridade de proteção de dados pessoais. Sobre este Decreto, interessa apontar, para os fins desta dissertação, que este reconhece em seu preâmbulo ser apropriado ajustar o sistema jurídico nacional aos regimes comparáveis mais aceitos, essencialmente aqueles estabelecidos pelos países da Europa por meio da Diretiva 95/46/CE.

A Comissão também destaca que em certos temas existem dispositivos em outras leis mais específicas que regulam certos tipos de banco de dados, sendo exemplificado como os

bancos de dados de registros públicos, de escrituras notariais, propriedade industrial e marca registrada, atos pessoais, direitos reais, mineração e análise de crédito. A relação de aplicação entre a Lei de dados pessoais e as disposições específicas se dá de forma supletiva, isto é, a Lei de dados se aplica na medida em que as atividades não sejam governadas pelo dispositivo específico que regula o banco de dados em questão. Apesar de ser um tema de extrema importância a compreensão de como os tipos de bancos de dados são regulados no país para que, de fato, possa-se ter uma avaliação adequada sobre o nível de proteção assegurado, a Comissão não adentra nesta questão.

Assim, a decisão se limita a apontar que a aplicação dos padrões é assegurada por meio de remédios judiciais e administrativos, em especial, o *habeas data*, que permite o titular de dados a levar o controlador ao Tribunal com a finalidade de garantir seus direitos de acesso, retificação e deleção. Ademais, existe a previsão de uma supervisão independente por meio da *Unidad Reguladora y de Control de Datos Personales* (URCDP). Trata-se de autoridade, conforme apontado pela decisão, com poderes de investigação, intervenção e sanção, de acordo com o artigo 28 da Diretiva, e que age de forma completamente independente. Ademais, qualquer parte interessada que sofra com o tratamento ilegal de dados pessoais pode procurar proteção judicial para compensação de eventuais danos.

Ainda sobre a forma de proteção dos dados pessoais, a decisão destaca que (i) quando a lei de proteção de dados do Uruguai não exige o consentimento para autorização da atividade de tratamento, ainda assim se exige cumprimento com princípio da transparência, proporcionalidade e finalidade (no caso da transparência, a decisão destaca que esta recai na obrigação de prestar informações aos titulares e se aplica em todas as situações); (ii) o direito de acesso é garantido bastando a comprovação da identidade no momento de apresentar o pedido e (iii) as exceções contidas na lei de proteção de dados ao princípio da transferência internacional não podem ser interpretadas de forma mais ampla do que o regime previsto no artigo 26 da Diretiva 95/46/CE.

No que toca aos compromissos internacionais, a Comissão considerou relevante que o Uruguai é parte da Convenção Americana de Direitos Humanos - CADH (Pacto São José da Costa Rica), de 22 de novembro de 1969, e em vigor desde 18 de julho de 1978. O artigo 11 da CADH estabelece que o direito à privacidade e o artigo 30 determina as restrições que os direitos e liberdades contidos na CADH podem sofrer. Neste sentido, exceções devem estar contidas em legislação e alinhadas a razões de interesse geral e de acordo com a finalidade para que as exceções foram criadas. O Uruguai também aceitou a jurisdição da Corte Interamericana de Direitos Humanos e foi convidado a aceder à Convenção 108 e seu Protocolo Adicional, depois de opinião favorável do Comitê Consultivo e da 1118º reunião dos Delegados dos Ministros do Conselho da Europa, que ocorreu em 06 de julho de 2011.

Diante deste cenário, o Uruguai foi reconhecido como país que cobre todos os princípios necessários para um nível de proteção adequado, fornecendo exceções e limitações na medida necessária para proteger interesses públicos importantes.

Tabela 20 – Padrões de proteção

Padrão Global	**Padrão Europeu**
- Qualidade dos dados, os quais devem ser relevantes, precisos e atualizados - Direito individual de acesso - Direito individual de correção - Transparência nas práticas de proteção de dados pessoais - Finalidade específica no momento da coleta	- Autoridade de proteção de dados independente - Recursos aos tribunais para fins de *enforcement* dos direitos dos titulares - Deleção (inserido dentro do primeiro critério do padrão de destruição ou anonimização de dados pessoais depois de um certo período) - Restrição às exportações de dados pessoais para países que não possuem padrão adequado de proteção da privacidade

4.2 Estados Unidos: o ponto fora do padrão das decisões emitidas sob a Diretiva

4.2.1 Contexto e panorama da Decisão de Adequação

A decisão que avalia o nível de proteção dos Estados Unidos destoa das demais que foram proferidas sob a vigência da Diretiva 95/46/CE. Em primeiro lugar, a decisão possui 36 páginas (cobertura maior do que as demais até aqui avaliadas), o que parece sinalizar um maior aprofundamento nas questões envolvendo os critérios e forma de implementação das regras e direitos de proteção de dados pessoais. Isto ainda é complementado pelos diversos Anexos que subsidiam e orientam a decisão em vários pontos. Os anexos compreendem (i) cartas do Secretário do Comércio, Secretário do Estado, do Secretário de Transporte, Subsecretário do Comércio Internacional dos EUA, da Comissão Federal de Comércio, do Conselheiro Geral do Escritório do Diretor de Inteligência Nacional, do Vice Procurador-Geral Adjunto e Conselheiro para assuntos internacionais; (ii) os princípios sob o *Privacy Shield*; (iii) o Modelo Arbitral sob o *Privacy Shield*; (iii) contexto e panorama da segurança dos EUA.

Em segundo lugar, podemos destacar que a Comissão Europeia teve o cuidado de expressamente estabelecer quais os princípios que devem ser assegurados na relação entre UE-EUA, enquanto nas demais decisões proferidas até então, ela somente se referia de forma genérica que os princípios garantiam um nível adequado de proteção, sem mencionar a quais princípios de fato a Comissão Europeia estava fazendo referência.

Ademais, nesta decisão fica definido de forma expressa o modelo de supervisão a ser desempenhado pelo FTC, Departamento de Comércio e Departamento de Transporte dos Estados

Unidos. Apesar de pouco tratar a respeito das características da autoridade independente nos moldes do padrão europeu de proteção, a Comissão reconhece e se aprofunda nas atribuições do Departamento do Comércio, FTC e Departamento do Transporte. O primeiro fica responsável pelo monitoramento do Acordo, sendo o órgão em que as empresas renovam sua certificação anualmente. O FTC e o Departamento do Transporte, por sua vez, possuem poderes executórios. Adicionalmente, a Comissão Europeia também discorre acerca de vias e procedimentos disponíveis aos titulares para reclamação e resolução de conflitos, passando por possibilidade de implementação de canais pela própria empresa até para a possibilidade de interação com órgãos fiscalizadores e pelo auxílio aos europeus prestados pelas autoridades de controle nacionais.

De forma inédita, a decisão percorreu as implicações, limites e cautelas necessárias em relação a acesso a dados por autoridades públicas. Assunto que não surgiu de modo detalhado e aprofundado – como um problema ou empecilho – até esta decisão. A decisão endereçava como preocupação central as atividades de vigilância massiva de inteligências de autoridades americanas, as quais colocavam em risco a privacidade e proteção dos dados pessoais dos dados vindos da União Europeia. Devido ao limite temático desta dissertação, este capítulo não trata das regras específicas do Acordo que justificam o acesso a dados por autoridades públicas. O tema se mostra de tamanha relevância que justifica outra linha condutora de pesquisa.

Convém destacar, no entanto, que esta preocupação foi central para que a relação entre EUA-EU enfraquecesse o Acordo *Safe Harbor*, culminando na sua invalidação pelo TJUE e passa a ser acordado de forma específica no âmbito do Acordo do *Privacy Shield*, visto ser condição necessária para que o novo Acordo apresente um nível adequado de proteção.

Por fim, a decisão de adequação faz ressalva importante ao estabelecer que o *Privacy Shield* não se aplica àquelas empresas cujas atividades de tratamento já esteja sob o escopo de aplicação da legislação da União Europeia. Trata-se, portanto, de aplicação de cunho subsidiário, uma vez que as atividades não recaiam dentro dos critérios de aplicação da Diretiva (e atualmente sob a aplicação completa do GDPR), então as empresas podem se valer da autocertificação e se adequar às exigências do *Privacy Shield*[3].

4.2.2 Critério material

Em relação aos princípios, a decisão de adequação esclarece que o *Privacy Shield*, à similaridade do antigo *Safe Harbor*, se aplica àquelas empresas autocertificadas, em que organizações estabelecidas nos Estados Unidos se comprometem a implementar determinados princípios, EU-US *Privacy Shield Framework Principles*, incluindo os Princípios Complementares (*Supplemental Principles*), em conjunto chamados de Princípios. Estes Princípios se aplicam às atividades de tratamento conduzidas pelos controladores e operadores de dados pessoais,

[3] Esta observação é importante visto que a decisão de adequação é uma entre as demais bases legais autorizadoras da transferência, bem como não faz sentido requerer que a empresa esteja certificada no regime do *Privacy Shield* quando esta já esteja sob o âmbito de aplicação da Diretiva ou, agora, do GDPR – cujo regime de tratamento é, portanto, o mesmo daquelas estabelecidas na UE.

com a especificidade de que os operadores devem estar contratualmente vinculados a agir de modo estritamente atrelado às instruções dada pelo controlador, bem como deve dar suporte ao controlador europeu para implementar os direitos dos titulares[4].

Apesar da decisão de adequação reconhecer que os Estados Unidos e União Europeia compartilham do objetivo de proteção à privacidade, esta ressalta que os Estados Unidos possuem uma abordagem diferente, a qual é descrita pela sua regulamentação fragmentada e pela sua aplicação setorial. Devido às diferenças, a decisão afirma que o Departamento de Comércio emitiu os Princípios do *Privacy Shield* - incluindo os complementares - com o objetivo de promover, fomentar e desenvolver o comércio internacional. Segundo aponta, os princípios foram construídos em conjunto com a Comissão Europeia, indústria e outros atores de forma a facilitar o comércio entre União Europeia e Estados Unidos.

A decisão também estabelece os possíveis limites a serem aplicáveis à implementação dos Princípios às atividades de tratamento das empresas que recebem os dados transferidos da União Europeia. Nesse sentido, aponta para três possibilidades de restrição da implementação dos Princípios, sendo eles: (i) quando necessário para a segurança nacional, interesse público ou *law enforcement*; (ii) por meio de lei, ato normativo do governo ou jurisprudência em que há conflitos de obrigações ou autorizações explícitas, desde que, em exercendo tais autorizações, a organização demonstre que sua não conformidade com os princípios está limitada ao necessário para o cumprimento do legítimo interesse da autorização dada; (iii) se os efeitos da Diretiva ou de uma lei do Estado Membro permitem exceções ou derrogações, desde que estas exceções e derrogações possam ser aplicadas em contextos comparáveis.

No que se refere aos princípios, estes foram detalhados no Anexo III da decisão de adequação. A tabela abaixo busca sistematizar os Princípios e os Princípios Complementares, seguida pela explicação de cada um deles.

Tabela 21 – Princípios do *Privacy Shield*

Princípios	Informação/aviso; escolha; responsabilização em casos de transferência subsequente; segurança; integridade dos dados e finalidade limitada; acesso; recurso, aplicação (*enforcement*) e responsabilidade;

[4] "The EU-U.S. Privacy Shield is based on a system of self-certification by which U.S. organisations commit to a set of privacy principles — the EU-U.S. Privacy Shield Framework Principles, including the Supplemental Principles (hereinafter together: 'the Principles') — issued by the U.S. Department of Commerce and contained in Annex II to this decision. It applies to both controllers and processors (agents), with the specificity that processors must be contractually bound to act only on instructions from the EU controller and assist the latter in responding to individuals exercising their rights under the Principles."(COMISSÃO EUROPEIA, 2016, p. 3).

Princípios Complementares	Dados sensíveis; exceções ao jornalismo; responsabilidade secundária; dever de diligência e de conduzir auditorias; o papel da autoridade de proteção de dados; autocertificação; verificação; acesso; recursos humanos; contratos obrigatório para transferências subsequentes; resolução de disputas e *enforcement*; escolha – tempo do *opt-out*; informação de viagem; produtos médicos e farmacêuticos; registro público e informação de disponibilidade pública; requisição de acesso por autoridades públicas.

a) Informação/Aviso

Fica estabelecido a necessidade da organização autocertificada de informar os indivíduos sobre (i) a sua participação no *Privacy Shield* e o respectivo link para a lista do *Privacy Shield*; (ii) os tipos de dados pessoais coletados e, quando aplicado, as entidades ou subsidiárias da organização que aderem aos Princípios; (iii) seu comprometimento com os princípios em relação a todos os dados recebidos da União Europeia; (iv) as finalidades pelas quais a empresa coleta e usa os dados pessoais; (v) como contatar a organização com dúvidas ou reclamações (incluindo qualquer estabelecimento relevante da União Europeia que possa responder às perguntas e reclamações); (vi) o tipo ou identidade de partes terceiras em que se divulga informações pessoais e a finalidade pela qual se justifica a atividade (vii) os direitos dos titulares; (viii) as escolhas e os meios que a empresa oferece aos indivíduos para limitarem o uso e divulgação de seus dados; (ix) o órgão independente de resolução de conflito designado para resolver questões de reclamações e fornecer recursos apropriados e gratuito aos indivíduos; (x) estar sujeito aos poderes investigativos e de *enforcement* do FTC, do Departamento de Transporte ou qualquer outro órgão autorizado em lei; (xi) a possibilidade do indivíduo de invocar arbitragem; (xii) as hipóteses de divulgação de informação pessoal em resposta a um pedido de autoridade pública, incluindo para cumprir com critérios de segurança nacional e *law enforcement*; (xiii) sua responsabilidade em caso de transferência de dados a terceiros.

No que toca o momento de disponibilização da informação, o Anexo estabelece como necessário que seja executado no primeiro momento em que é feita a coleta dos dados pessoais, por meio de linguagem clara.

b) Escolha

As organizações devem oferecer aos indivíduos a opção de *opt-out* (opor-se) se suas informações forem (i) divulgadas a parte terceiras; (ii) usadas para uma finalidade que seja materialmente diferente das finalidades em que foram originalmente coletadas ou subsequentemente autorizadas pelo indivíduo. O *opt-out* para o compartilhamento não se aplica na relação entre controlador-operador (casos em que o operador age de acordo com as instruções do primeiro). Para os casos de dados sensíveis, as organizações devem obter consentimento expresso (*opt-in*) dos indivíduos se a informação for (i) divulgada a partes terceiras ou (ii) usadas para finalidade outras que não a originalmente coletadas ou subsequentemente autorizadas.

c) Responsabilização em casos de transferência subsequente

A regra geral é que a todos os terceiros que intervenham no tratamento de dados, independente da localização (se localizado no território dos EUA ou em demais países), devem fornecer mesmo nível de proteção que aquele garantido pelos princípios.

Para que seja possível transferir qualquer informação a terceiro controlador, organizações devem se comprometer com os deveres de informar e de oferecer escolha aos titulares (permitindo aos titulares da União Europeia que façam o *opt-out*). Deve-se também estipular contrato com os terceiros controladores especificando que estes dados sejam tratados para finalidades limitadas e específicas, consistente com o consentimento fornecido pelo indivíduo e que o receptor fornecerá o mesmo nível de proteção conferido pelos Princípios. Caso o agente receptor não cumpra mais com suas obrigações, deve então notificar a outra parte e cessar ou buscar medidas razoáveis e apropriadas para remediar a situação.

Por fim, a decisão de adequação permitiu uma exceção no que se refere às relações contratuais e sua conformidade com os princípios: considerando a dificuldade de trazer todos os parceiros comerciais em conformidade com os princípios do *Privacy Shield*, as organizações ficaram obrigadas a assim fazer o mais rápido possível ou respeitado até nove meses a partir da autocertificação (desde que a autocertificação tenha sido feita até dois meses da aprovação do *Privacy Shield*).

d) Segurança

As organizações devem tomar medidas razoáveis e apropriadas para proteger de perda, mau uso, acesso, divulgação, alteração e destruição não autorizadas, tomando em consideração os riscos envolvendo a atividade de tratamento e os tipos de dados pessoais. A decisão também prevê que em caso de tratamento ulterior deve-se celebrar contrato com a organização receptora dos dados de forma a garantir que esta implemente medidas para assegurar o nível de proteção e aplicação adequada das técnicas de segurança.

e) Integridade dos dados e finalidade limitada

Os dados pessoais devem ser limitados para a finalidade do tratamento. A organização não pode tratar dados pessoais de modo incompatível com as finalidades pelas quais foram originalmente coletados ou subsequentemente autorizados pelos titulares de dados. Os dados devem ser exatos, completos e atuais. Uma organização deve cumprir com os princípios enquanto mantenha/retenha esses dados. Exceção a esta regra se aplica em casos de tratamento cuja finalidade seja de reter os dados por conta de interesse público, jornalismo, literatura, arte, ciência ou pesquisa histórica e análise estatística. Nestes casos, deve-se ainda cumprir com os demais princípios.

f) Acesso

Os indivíduos devem ter acesso aos dados pessoais mantidos pelas organizações, assim como de serem capazes de corrigir, emendar, deletar a informação quando incorretos, ou tenham sido tratados em violação aos princípios. Exceção pode ocorrer quando considerados desproporcionais os custos relacionados ao pedido em relação ao risco da privacidade do indivíduo em questão ou quando os direitos de terceiros sejam violados.

Este direito deve ser garantido sem a necessidade de apresentar justificativa e sem que se imponha uma taxa excessiva. A negativa para o cumprimento deste direito pela organização deve ser devidamente justificada.

De forma adicional, o Anexo ressalta sobre o tratamento automatizado de dados pessoais cuja finalidade é obter uma decisão que afeta o titular (como nos casos de concessão de crédito e emprego). Neste âmbito, a Comissão esclarece que o direito dos Estados Unidos proporciona proteções específicas contra as decisões negativas, as quais abrangem (i) direito de informação das razões específicas que embasaram a decisão; (ii) de contestar as informações incompletas e inexatas e (iii) procurar reparação.

Com o aumento da importância da tomada de decisão automatizada, a Comissão Europeia ressalta a necessidade de que este tema venha a ser acompanhado de perto pelas autoridades europeias e americanas, por meio de diálogo e intercâmbio sobre as semelhanças e diferenças das abordagens adotadas pela UE e Estados Unidos. Esta troca deve repercutir na primeira análise anual do Acordo e nas próximas, caso necessário.

g) Recurso, aplicação (*enforcement*) e responsabilidade

Neste ponto, a Comissão ressalta que, apesar da decisão da autocertificação ser voluntária, o cumprimento dos Princípios após certificadas é obrigatório. Assim, para que a proteção da privacidade possa ser efetiva, as organizações devem fornecer mecanismos robustos garantindo a conformidade, recursos aos indivíduos afetados pela não conformidade com os Princípios e o sistema deve prever consequências para a organização quando os Princípios não sejam cumpridos.

Em relação aos mecanismos robustos, aponta-se que as organizações devem garantir, no mínimo, o seguinte: (i) canal disponível para reclamações, sendo as disputas investiga-

das e resolvidas sem nenhum custo e com fundamento nos Princípios, bem como com devido ressarcimento de danos; (ii) procedimento para verificação de que os atestados e certificações da organização realmente representam suas práticas de privacidade, por meio de reexames periódicos de forma objetiva ou verificações de conformidade externas, por meio de auditorias ou verificações aleatórias; (iii) obrigações para remediar problemas que surgem com a não conformidade da organização.

As sanções devem ser suficientemente rigorosas para garantir a conformidade das organizações. No contexto de transferências subsequentes, a organização tem responsabilidade em relação às atividades de tratamento desenvolvidas pelos operadores (que agem eu seu nome e sob suas instruções), salvo quando a organização provar que não foi responsável pelo evento que deu causa ao dano.

h) Princípios complementares

No que toca aos princípios complementares, convém destacar seis deles pois são aqueles que importam para a análise em relação aos critérios de padrão de proteção europeu e global (lente de análise estipulada para leitura das decisões). São eles: dados sensíveis, acesso, contratos obrigatórios para transferências subsequentes, escolha – *opt-out*.

No que se refere aos dados sensíveis, para além da necessidade de se obter o consentimento expresso (*opt-in*) para tratamento de dado sensíveis, o Anexo III da decisão de adequação estipula as hipóteses possíveis que configuram a exceção ao consentimento. São elas possíveis em caso de (i) função de interesses vitais da pessoa em causa ou de outra pessoa; (ii) preparação de recursos ou processos judiciais; (iii) cuidados médicos ou elaborar um diagnóstico; (iii) decurso das atividades legítimas de uma fundação, associação ou qualquer outro organismo sem fins lucrativos que possua objetivos políticos, filosóficos, religiosos ou sindicais, na condição de que o tratamento se refira exclusivamente aos membros do organismo ou às pessoas que com ele mantenham contatos habituais no âmbito dos referidos objetivos, e de que os dados não sejam revelados a terceiros sem o consentimento dos titulares de dados; (iv) necessidade de cumprimento das obrigações em matéria de direito do trabalho ou (v) se referir à informação publicada pela pessoa em causa.

Em relação à implementação do direito de acesso, este não deve ser condicionado à apresentação de justificativa e deve abranger a confirmação do tratamento, a disponibilidade dos dados a fim de que o titular possa verificar sua exatidão e a legalidade do tratamento, bem como proceder com eventual pedido de correção, alteração e eliminação quando incorretos ou que estejam sendo tratados em infração a algum princípio. A Comissão ainda esclarece que caso o pedido seja considerado muito vago, cabe à empresa estabelecer um canal de comunicação com o titular de forma a compreender qual a motivação do pedido e prestar as informações adequadas. Nos casos em que os dados sejam facilmente

distinguidos de outros dados pessoais, deve a empresa reter a informação pessoal e disponibilizar o dado que diz respeito ao solicitante.

Ainda pode ser objeto de indeferimento do pedido de acesso quando uma organização entenda que o acesso implica em revelações de informações comerciais confidenciais a seu respeito, como pode ser considerado nos casos em que é feito deduções ou classificações de marketing ou informações confidenciais de terceiros partes de uma obrigação contratual de confidencialidade. No entanto, à similaridade do primeiro caso, quando a informação for passível de ser distinta com facilidade da informação confidencial, a empresa deve reter esta última e disponibilizar as informações pessoais solicitadas. O direito de acesso é oponível pelo titular a medida em que aquela organização mantenha seus dados, não se trata de direito que impõe uma obrigação às empresas de manutenção de dados visto a potencialidade de um pedido do titular.

Por fim, a decisão reconhece o direito de *opt-out* para os casos de tratamento de dados com finalidade de marketing direto.

4.2.3 Critério procedimental

Em relação ao modelo de supervisão, a decisão de adequação confere responsabilidade de monitoramento e fiscalização de conformidade das empresas autocertificadas ao Departamento de Comércio, FTC e Departamento do Transporte.

Em relação ao Departamento de Comércio, este fica responsável pela (i) verificação de conformidade ao Acordo, envidando esforços para identificar falsas alegações de autocertificação; (ii) compromisso de disponibilizar ao público lista oficial atualizada de organizações dos EUA que declaram a sua adesão, sendo que em caso de supressão de alguma organização, o Departamento deve informar ao público que esta organização ainda está vinculada ao Acordo em relação aos dados pessoais que receberam durante sua participação e enquanto conservam tais dados; (ii) mediante pedido, pode obter cópia de disposições relevantes em contratos com agentes de tratamento celebrados pelas empresas autocertificadas; (iii) gerenciamento da celeridade de resposta das organizações às queixas relativas à conformidade do tratamento; (iv) fornecimento de informação dos casos da FTC relacionados ao Acordo apresentados no site do FTC.

O Anexo 01 – Carta do Subsecretário interino para as questões do comércio internacional ainda estabelece que o Departamento de Comércio possui atuação importante no auxílio às autoridades de proteção de dados da União Europeia (chamadas no Anexo de APD). O Anexo prevê forma de cooperação entre as autoridades para auxílio nas queixas de um cidadão de combate à alegação falsa de autocertificação.

Ao FTC e Departamento do Transporte cabe a função de aplicação dos princípios, assegurando o cumprimento efetivo por parte das empresas autocertificadas (*enforcement*). Nesse sentido, estes órgãos possuem função de investigação a respeito das declarações falsas prestadas

ao Departamento de Comércio, passíveis de execução segundo o que dispõe o *False Statements Act* (legislação sobre falsas declarações).

4.3 Japão: a primeira decisão sob o GDPR

4.3.1 Contexto e panorama da Decisão de Adequação

A decisão de adequação proferida pela Comissão Europeia em relação ao Japão, de 23 de janeiro de 2019, é a primeira sob a vigência do GDPR. Trata-se de decisão que reconhece o nível de adequação das relações estabelecidas no âmbito de aplicação da Lei relativa à proteção de informações pessoais (APPI) do Japão, bem como que estejam sujeitas às condições adicionais estabelecidas na decisão. As condições adicionais se encontram nos Anexos da decisão e podem ser definidas como as normas complementares adotadas pela Comissão de Proteção de Informações Pessoais (PPC) e as declarações, garantias e compromissos oficiais assumidos pelo Governo japonês à Comissão Europeia.

As normas complementares adotadas pelo PPC se aplicam na relação de transferência internacional entre União Europeia e Japão e são consideradas mais rígidas do que aquelas contidas na APPI. Ainda, conforme consta na decisão, estas regras possuem força legal perante os operadores comerciais japoneses e são passíveis de execução tanto pela PPC como pelos Tribunais. No Anexo I da decisão, fica esclarecido que o artigo 6º da APPI prevê a possibilidade de se adotarem medidas legislativas ou de outro tipo (como no caso presente) para reforçar a proteção das informações pessoais e criar um sistema compatível com as normas internacionais, incluindo regras mais rigorosas que complementem e amplifiquem o que disposto na Lei e no Decreto ministerial (que versam sobre o tema no sistema jurídico do Japão).

Conforme se vê, a decisão não se estende a todo o Japão, mas limita-se ao âmbito de aplicação da APPI, cuja proteção cobre as informações pessoais tratadas pelos "operadores comerciais responsáveis pela gestão de informações pessoais" (do inglês *Personal Information Handling Business Operators* - PIHBO), segundo os termos estabelecidos na APPI. Nesse quesito, fica de fora da cobertura da legislação e, portanto, da decisão de adequação, as entidades do setor público, as quais são reguladas de forma apartada por legislação específica, chamadas de Lei relativa à proteção de informações pessoais na posse de órgãos administrativos (APPIHAO) e Lei relativa à proteção de informações pessoais na posse de serviços administrativos legalmente constituídos (APPI-IAA).

Dito o âmbito de cobertura da decisão proferida pela Comissão Europeia ao Japão, destaca-se que a decisão passa pelo quadro normativo do sistema jurídico do Japão, evidenciando que este rege a privacidade e a proteção dos dados pessoais tendo como origem sua Constituição, promulgada em 1946. Apesar desta não prever de forma expressa ambos direitos, a decisão ressalta que o Supremo Tribunal japonês esclareceu o que está abrangido dentro dos direitos

individuais constitucionais.

Assim, em decisão proferida em 1969, a Comissão Europeia destaca que o Supremo Tribunal entendeu que os "indivíduos têm a liberdade de proteger as suas informações pessoais contra a transmissão a terceiros ou a divulgação pública sem motivo justificado" (p.02). Em 2008, o Supremo Tribunal reconheceu que "a liberdade dos cidadãos na vida privada deve ser protegida contra o exercício da autoridade pública e que pode entender-se, como uma das liberdades individuais na vida privada, que cada indivíduo tem a liberdade de proteger as suas informações pessoais contra a transmissão a terceiros ou a divulgação pública sem motivo justificado" (p.02).

Em relação à APPI, esta foi alterada em 2015 e suas alterações entraram em vigor em 30 de maio de 2017. A alteração introduziu, segundo palavras da Comissão Europeia, garantias mais semelhantes àquelas contidas no sistema da União Europeia. Dentre elas, um conjunto de direitos individuais oponíveis e a criação de uma autoridade de controle independente (o então PPC), responsável pela supervisão e aplicação coerciva da APPI.

Dentre as observações feitas no âmbito de aplicação material da APPI, convém aqui destacar que a Comissão observa que a APPI difere o conceito de informações pessoais de dados pessoais. Em relação ao conceito de informação pessoal, a APPI define como toda e qualquer informação relacionada a uma pessoa viva que permita a sua identificação. Dentro deste conceito, estão englobadas duas categorias (i) códigos de identificação individuais e (ii) outras informações pessoais pelas quais uma determinada pessoa singular pode ser identificada. Nesta última categoria, se encaixam aquelas informações que por si só não identificam uma pessoa, mas quando agrupadas com outras permitem a identificação. Trata-se aqui, como se vê, de uma aproximação do conceito expansionista de dados pessoais (identificada ou identificável).

Em relação à informação que precisa ser agrupada para identificar o indivíduo, o PPC ressalta que esta informação deve ser considerada pessoal desde que não demande esforços inusitados ou o agente tenha de cometer atos ilegais para as obter junto de outros operadores comerciais. Todavia, esta avaliação, conforme ressaltado pelo PPC, depende de uma abordagem caso a caso.

O conceito de dados pessoais, por sua vez, diz respeito às informações pessoais que constituem uma base de dados de informações pessoais, sendo sistematicamente organizadas para que seja possível pesquisar informações pessoais por meio de computador. Contudo, é possível haver derrogações a esta regra previstas em Decreto ministerial. Segundo a decisão, o PPC esclarece que há exceção prevista para as listas telefônicas e outros tipos de listas semelhantes.

Do ponto de vista prático, a diferenciação está no conjunto de regras aplicáveis às informações coletadas manualmente, por exemplo, daquelas que compõe base de dados computadorizadas. No que toca à relação estabelecida entre UE e Japão, a Comissão ressalta que esta diferenciação não tem tamanha relevância visto que os dados internacionais são principalmente transferidos por meio eletrônico. Neste sentido:

> Em contrapartida, esta distinção não é relevante no caso de dados pessoais importados da União Europeia para o Japão com base numa decisão de adequação. Dado que esses dados são normalmente transferidos por meios eletrónicos (pois, na presente era digital, é esse é o modo habitual de intercâmbio de dados, especialmente nas grandes distâncias, como sucede entre a UE e o Japão), passando, por conseguinte, a fazer parte do sistema de arquivo eletrónico do importador dos dados, nos termos da APPI, esses dados da UE enquadram-se na categoria de «dados pessoais». No caso excecional de os dados pessoais serem transferidos da UE por outros meios (por exemplo, em suporte de papel), continuarão a ser abrangidos pela APPI se, após a transferência, passarem a fazer parte de um «conjunto global de informações» sistematicamente organizadas de modo a permitir uma pesquisa fácil de informações específicas [artigo 2, n. 4, alínea ii) da APPI]. Nos termos do artigo 3, n.2, do decreto ministerial, será esse o caso quando a informação estiver estruturada «de acordo com uma regra específica» e a base de dados contemplar instrumentos como um índice ou um índice remissivo para facilitar a pesquisa. Isto corresponde à definição de «ficheiro» na aceção do artigo 2, n. 1, do RGPD. (COMISSÃO EUROPEIA, 2019, p. 5)

Sobre o conceito de dados anonimizados, estes não foram considerados suficientes quando comparados com a proteção conferida pela União Europeia. Assim sendo, a Comissão explicitou em norma complementar que deve ser garantido que o processo de anonimização dos dados de titulares da UE seja conduzido no Japão em conformidade com o que disposto no GDPR. Nesse sentido, a Comissão entende que o conceito de anonimização da APPI se aproxima ao conceito de pseudonimização do GDPR, visto ser passível de reversão e recomenda, assim, a exclusão da chave de reidentificação dos dados pessoais pelos operadores, de forma a aproximar-se dos padrões europeus de proteção. Ressalta-se que no processo de pseudonimização, nos termos do GDPR, os dados ainda permanecem com a natureza de dados pessoais.

Em seguida, a Decisão ressalta que a APPI possui alguns âmbitos em que a legislação não se aplica. Esta exceção está prevista no artigo 76 da APPI, a qual elenca os tipos de tratamento de dados que não estão sujeitos ao cumprimento dos princípios básicos, obrigações dos operadores comerciais, direitos individuais e supervisão pela PPC. Nesta categoria estão inclusos setores específicos que tratem dados para uma finalidade determinada como (i) nos casos de radiodifusão, editores de jornais, agências de comunicação ou outros órgãos da imprensa, na medida em que tratem informações para efeitos de divulgação na imprensa; (ii) instituições religiosas e organismos políticos, na medida em que tratem informações pessoais para efeitos de suas respectivas atividades; (iii) universidades e ouras organizações ou grupos orientados para estudos acadêmicos ou pessoas singulares pertencentes a organizações desse tipo, na medida em que tratem informações pessoais para estudos acadêmicos; (iv) pessoas que se dedicam à atividade de escrita profissional, na medida em que envolva informações pessoais.

Por fim, convém destacar que a Comissão ressalta como deve ser tratada uma relação entre uma organização sujeita ao APPI e outra não sujeita. Deve-se, nestes casos, entender a relação como caso de transferência internacional de dados, na qual é necessário implementar as garantias adequadas para manutenção do nível de proteção dos dados. Vejamos:

> A fim de assegurar um nível de proteção adequado dos dados pessoais transferidos da União Europeia para operadores comerciais no Japão, somente o tratamento de informações pessoais abrangido pelo âmbito de aplicação do capítulo IV da APPI, ou seja, por um PIHBO na medida em que o tipo de tratamento não corresponda a uma das exclusões setoriais, deve ser abrangido pela presente decisão. O seu âmbito de aplicação deve, por conseguinte, ser harmonizado com o da APPI. Segundo as informações transmitidas pela PPC, se um PIHBO abrangido pela presente decisão alterar posteriormente a finalidade de utilização (na medida do permitido), passando esta a ser abrangida por uma das exclusões setoriais previstas no artigo 76 da APPI, tal deve ser considerado uma transferência internacional (na medida em que, nesses casos, o tratamento das informações pessoais deixa de ser abrangido pelo capítulo IV da APPI, saindo do respetivo âmbito de aplicação). O mesmo sucede caso um PIHBO forneça informações pessoais a uma entidade abrangida pelo artigo 76 da APPI, para serem utilizadas para uma das finalidades indicadas na referida disposição. No que respeita aos dados pessoais transferidos da União Europeia, tal constituiria, por conseguinte, uma transferência subsequente sujeita às garantias pertinentes (nomeadamente as especificadas no artigo 24 da APPI e na norma complementar 4. Quando o PIHBO deva obter primeiro o consentimento do titular dos dados (25), deve transmitir-lhe todas as informações necessárias, incluindo o facto de as informações pessoais deixarem de estar protegidas ao abrigo da APPI. (COMISSÃO EUROPEIA, 2019, p. 8)

4.3.2 Critério material

a) Limitação da finalidade

A partir desta regra, garante-se que o tratamento de dados pessoais ocorra mediante estipulação de uma finalidade específica. Os agentes de tratamento devem indicar a finalidade da forma mais explícita possível, não podendo alterar a finalidade inicial para além do âmbito reconhecido como razoavelmente pertinente para a finalidade de utilização anterior à alteração. Nesse sentido, o PPC esclarece que a mudança da finalidade pode ocorrer limitada ao que pode ser objetivamente esperado pelo titular com base em convenções sociais.

A Comissão ressalta dois exemplos dado pela PPC que representam um contexto em que a mudança da finalidade é aceita e outro contexto em que não se é razoavelmente aceita. O primeiro exemplo é dado no caso em que a informação é adquirida por meio de compra de bens ou serviços, em contexto de transação comercial, e a estas informações aplica-se outra finalidade de comunicação aos titulares a respeito da oferta de outros bens ou serviços pelo fornecedor. O segundo exemplo não contempla a possibilidade de mudança de finalidade nos casos em que uma empresa envia informações sobre oferta de bens e serviços para pessoas cujos dados foram fornecidos com a finalidade de alertar sobre a ocorrência de uma fraude ou furto de um cartão, por exemplo.

No que toca a mudança de finalidade de um dado originado na União Europeia e transmitido para o Japão, o operador comercial deve manter a finalidade estipulada no momento da coleta e para que haja uma alteração da finalidade em qualquer fase da cadeia de tratamento no Japão, exige-se o consentimento do titular dos dados da União Europeia. Assim, quando

não for possível contatar o titular dos dados, a consequência única é que o operador comercial mantenha a finalidade original da coleta.

b) Licitude e lealdade do tratamento

A licitude e lealdade do tratamento envolve regras para compartilhamento e a vedação de obtenção de dados de forma fraudulenta ou ilícita. Em relação ao compartilhamento, tem-se como regra geral a exigência de consentimento prévio do titular dos dados ou, nos casos de dados triviais, mediante cumprimento das derrogações do consentimento cumprindo a finalidade previamente estipulada. Segundo esta regra, os operadores comerciais devem confirmar a finalidade específica relacionada à transferência e tratar subsequentemente esses dados em conformidade com essas finalidades. Trata-se de vinculação da cadeia à atividade previamente estipulada.

c) Exatidão e minimização dos dados

Os dados devem ser exatos e, quando necessários, atualizados. No mesmo sentido, devem ser adequados, pertinentes e não excessivos relativamente às finalidades que são tratados. No que se refere ao dever de manter a exatidão dos dados, a Comissão Europeia ressalta que os operadores comerciais devem se esforçar para manter os dados exatos e atuais dentro do âmbito necessário para cumprir uma finalidade de utilização, sendo que o não cumprimento dos níveis de exatidão podem tornar a atividade ilícita.

d) Limitação da retenção

Não devem ser retidos por mais tempo do que o necessário para o cumprimento da finalidade que justifica o tratamento, resultando, assim, na obrigação de apagar os dados quando a utilização deixar de ser necessária. A decisão ressalta exceção no caso em que se obtém o consentimento do titular para tanto.

e) Segurança dos dados

Trata-se de proteção contra tratamento não autorizado ou ilícito e contra perda, destruição ou danos acidentais. Devem os operadores comerciais tomar as medidas técnicas e organizacionais adequadas para proteger os dados pessoais contra eventuais ameaças. A avaliação das medidas implementadas deve ocorrer levando em consideração o conhecimento e os custos relacionados ao contexto.

f) Transparência

Deve ser conferido ao titular informações a respeito do tratamento dos dados pessoais, como a respeito da coleta dos dados, finalidade do tratamento e compartilhamento. A transparência também recai nos casos de alteração da finalidade autorizada. Ademais, nos casos de compartilhamento de dados pessoais, a informação é condição necessária para que se possa proceder com a atividade.

As exceções cabíveis estão relacionadas a temas ligados a interesse público e proteção dos direitos e interesses do titular, de terceiros ou do responsável pelo tratamento. A título de exemplo, a Comissão destaca os casos de combate à fraude, espionagem industrial e sabotagem.

g) Categorias especiais de dados

Trata-se de informações a respeito de "raça, credo, estatuto social, historial clínico e registo criminal do titular, bem como o facto de ter sofrido danos em consequência de um crime, ou outras descrições, etc. determinadas por decreto ministerial como aquelas cujo tratamento requer atenção especial por forma a não causar discriminação injusta, prejuízo ou outras desvantagens ao titular" (COMISSÃO EUROPEIA, 2019, p. 11).

Em seguida, a Comissão passa a estabelecer as similaridades entre os conceitos de categorias especiais de dados com aqueles contidos no GDPR sobre o mesmo tema. Ressalta que não se trata de uma lista exaustiva, uma vez que mais dados podem ser incluídos a partir da possibilidade de levantar risco de discriminação injusta, prejuízo ou outras desvantagens ao titular. Sobre a possibilidade de que o Japão reconheça os dados sensíveis de acordo com o GDPR, a Comissão "conseguiu" que o Japão reconhecesse como sensíveis os dados que se encaixem no conceito dado pelo GDPR. Vejamos:

> Embora o conceito de dados «sensíveis» seja, por inerência, um conceito social no sentido em que se fundamenta nas tradições culturais e jurídicas, nas considerações morais, nas opções políticas, etc. de uma determinada sociedade, perante a importância de assegurar garantias adequadas para os dados sensíveis, quando transferidos para operadores comerciais no Japão, a Comissão conseguiu que as proteções especiais conferidas a «informações pessoais que requerem atenção especial», no âmbito da legislação japonesa, fossem alargadas a todas as categorias reconhecidas como «dados sensíveis» no Regulamento (UE) 2016/679. (COMISSÃO EUROPEIA, 2019, p. 11)

Interessante destacar, todavia, que a Comissão Europeia destaca na decisão que a categorização do que seja dado sensível é um tema inerente a um conceito social, fundado nas tradições culturais, jurídicas, morais e políticas de uma determinada sociedade. Dessa forma, ressalta que "conseguiu" o reconhecimento de que dos dados saídos da jurisdição europeia relacionados à vida sexual, orientação sexual ou filiação sindical sejam tratados como sensíveis dentro do contexto que se insere o tratamento deste dado no Japão.

Como garantia de proteção adicional, o tratamento deste tipo de dado pressupõe a obtenção do consentimento prévio do titular, com possibilidade de derrogações limitadas. A transmissão a terceiros também possui regime diferenciado daquele previsto aos dados triviais, sendo mais restrito.

h) Responsabilização

As entidades responsáveis pelo tratamento de dados são obrigadas a aplicar medidas técnicas e organizacionais adequadas de forma a cumprir com as obrigações de proteção de

dados pessoais. Nesse sentido, inclui-se a obrigação imposta aos operadores comerciais de verificar a identidade de um terceiro que lhes transmita dados pessoais, bem como verificar as circunstâncias nas quais os dados foram obtidos. Trata-se de medida que visa garantir a licitude dos dados ao longo da cadeia de tratamento. Os operadores comerciais devem, assim, manter registro a respeito da data de recepção dos dados, as informações recebidas do terceiro, a categoria de dados tratados e, quando cabível, o registro do consentimento do titular para o compartilhamento dos dados. Os registros devem ser conservados no período de um a três anos e podem ser exigidos pela PPC. Os operadores comerciais também devem tratar de forma célere e adequada as reclamações apresentadas por pessoas físicas afetadas quanto ao tratamento de suas informações.

i) Restrições relativas a transferências subsequentes

Dentre as regras relativas à transferência subsequente de dados pessoais, a lógica a ser aplicada é que a transferência que ocorra entre um operador comercial abrangido pela decisão de adequação e um terceiro mantenha o nível adequado de proteção dos dados pessoais. Assim, os destinatários localizados fora do território japonês devem estar sujeitos a regras que assegurem um nível de proteção semelhante ao garantido no âmbito da ordem jurídica japonesa.

A regra vigente no Japão sobre a possibilidade de transferência de dados a países terceiros é de que esta atividade é proibida, de modo geral, sem o consentimento prévio do titular. A Comissão, em norma complementar, exige que o consentimento obtido do titular da UE seja informado sobre as circunstâncias inerentes à transferência, dentre elas especificando que os dados serão transferidos para o estrangeiro (fora do âmbito de aplicação da APPI), assim como sobre qual o país de destino, permitindo que o titular avalie o risco da sua privacidade relacionado à transferência. Outras duas informações a serem providenciadas são em relação à categoria dos dados fornecidos a terceiros e o método de divulgação.

A regra do consentimento apresenta certas derrogações, como nos casos em que a PPC reconhece o país terceiro com nível de proteção equivalente ao do Japão ou quando o operador comercial e o destinatário no país terceiro adotaram conjuntamente medidas que garantem o nível de proteção equivalente ao da APPI, por meio de contrato, acordos vinculativos, convenções vinculativas no âmbito de um grupo de empresas. Conforme apontado pela própria Comissão, a segunda categoria corresponde aos instrumentos do GDPR de cláusulas contratuais e normas globais corporativas – BCRs.

A Comissão ressalta que não estão abrangidos como hipóteses autorizadoras da transferência o fato de que Japão faz parte do sistema das regras da APEC de proteção de dados. Isto se dá porque as relações que ocorrem neste sistema não vinculam importador e exportador de dados pessoais diretamente, assim como apresentam um nível inferior de proteção quando comparado às regras da APPI e das normas complementares (a título

de exemplo, a Comissão Europeia cita a ausência de definição de dados sensíveis e de proteção especificas a serem conferidas aos dados desta natureza).

j) Direitos individuais

A decisão evidencia que a APPI garante o direito de acesso, retificação e apagamento, bem como o de oposição. Contudo, em relação a este último, a Comissão ressalta que a APPI não garante o direito de oposição para marketing direto. Ocorre que em hipótese alguma a Comissão entende possível flexibilizar esta regra ao tratamento dos dados de titulares da UE. Vejamos:

> Ao contrário do direito da UE, a APPI e as normas legais acessórias pertinentes não contêm disposições jurídicas que abordem especificamente a possibilidade de oposição para efeitos de comercialização direta. Esse tratamento deve, contudo, por força da presente decisão, ter lugar no quadro de uma transferência de dados pessoais previamente recolhidos na União Europeia. Nos termos do artigo 21, n. 2, do Regulamento (UE) 2016/679, o titular dos dados deve ter sempre o direito de se opor a uma transferência de dados destinados a tratamento para efeitos de comercialização direta. (COMISSÃO EUROPEIA, 2019, p. 15)

Os operadores comerciais devem notificar o titular a respeito do andamento de seus pedidos, apresentando justificativa para eventual recusa. A implementação deste direito pode estar condicionada a taxas desde que o seu valor esteja dentro do considerado razoável tendo em consideração os custos reais envolvidos.

Em relação ao tratamento automatizado de dados pessoais, a Comissão ressalta que a APPI não contém disposições gerais que contemplem a questão. O Japão possui algumas normas setoriais nesse sentido, como no caso do setor financeiro, em que o assunto é direcionado pelas "Orientações abrangentes relativas à supervisão dos principais bancos", revista em 2017, a qual prevê a possibilidade de explicação da decisão ao titular de dados no que toca às razões do indeferimento do seu pedido para celebrar um acordo de empréstimo.

Nesta questão, a Comissão entendeu que a ausência de explicação de decisão automatizada não prejudicaria o nível de proteção adequado visto que o responsável pelo tratamento dos dados, o qual teria a ligação direta com o titular, estaria na União sendo a ele, portanto, aplicável o GDPR. Vejamos:

> Em qualquer caso, no que se refere aos dados pessoais recolhidos na União Europeia, qualquer decisão baseada num tratamento automatizado será, normalmente, tomada pelo responsável pelo tratamento dos dados na União (que tem uma relação direta com o titular dos dados em causa), estando, por conseguinte, sujeita ao Regulamento (UE) 2016/679. Tal inclui cenários de transferência em que o tratamento seja realizado por um operador comercial estrangeiro (por exemplo, japonês), que atua como agente (subcontratante) do responsável pelo trata mento da UE (ou como subcontratante ulterior do subcontratante da UE, o qual por sua vez recebeu os dados de um responsável pelo tratamento da UE que os recolheu) que, nesta base, toma então a decisão. Deste modo, não é provável que a inexistência na APPI de regras específicas sobre a tomada

> de decisões automatizadas afete o nível de proteção dos dados pessoais transferidos ao abrigo da presente decisão. (COMISSÃO EUROPEIA, 2019, p. 16)

4.3.3 Critério procedimental

No que se refere ao tópico de supervisão e execução coerciva, a Comissão ressalta a necessidade de se criar uma autoridade de controle independente, com poderes de supervisão e aplicação coerciva das normas em matéria de proteção de dados. A independência e imparcialidade são requisitos necessários à forma da autoridade. Convém destacar aqui as seguintes características da autoridade japonesa (PPC) que são destacadas na decisão da Comissão, como: (i) constituição da autoridade por meio de um presidente e oito comissários, designados pelo primeiro-ministro mediante aprovação de ambas as câmaras da Dieta (do inglês *Houses of the Diet*); (ii) o presidente e o comissário possuem mandato de cinco anos com a possibilidade de recondução; (iii) os comissários só podem ser destituídos por justa causa; (iv) os comissários não podem se envolver em atividades políticas; (v) devem abster-se de exercer outras atividades remuneradas ou de caráter comercial.

Dentre suas competências, a Comissão ressalta que o PPC pode proceder com inspeções no local do tratamento ou em relação aos documentos, pode solicitar ao agente de tratamento a comunicação de informações ou apresentação de documentos. A autoridade tem também função de orientação em relação às atividades desenvolvidas pelos agentes de tratamento (PIHBO), bem como pode dar prosseguimento a queixa ou atuar por sua própria iniciativa para emitir recomendações e ordens destinadas à aplicação da APPI e outras normas vinculativas em casos concretos. Conforme consta na decisão, a PPI já exerceu esta última função no caso de orientações dirigidas ao Facebook, quando das revelações ocorridas no caso Cambridge Analytica.

No que toca o sistema de reclamações oferecidos pelo Japão, a este é possível opor reclamação diretamente ao agente de tratamento de dados pessoais (PIHBO), o qual deve envidar esforços para tratar tais reclamações, de forma célere e estabelecer sistemas internos de tratamento de reclamações para atingir esse objetivo. A Comissão ressalta que o legislador japonês confiou aos órgãos de poder local atribuição para assegurar a mediação dessas reclamações, sendo possível ao titular apresentar reclamação junto de mais de 1700 centros do consumidor ou junto do Centro Nacional para os Assuntos do Consumidor do Japão.

Em relação às vias disponíveis ao titular, a decisão destaca que está à disposição do titular vias judiciais no âmbito cível e penal em relação ao agente do tratamento. No âmbito civil, ocorre a aplicação do Código Civil do Japão mediante o que dispõe as regras de responsabilidade civil, sendo necessário comprovar culpa – dolo ou negligência – e danos materiais ou morais. Tais ações podem resultar em indenizações ou em ordem inibitória destinada a por fim ao tratamento ilícito. Sobre os casos em que o operador comercial incorra em descumprimento de uma ordem da PPC, esta conduta é tida como infração penal e pode resultar em pena de prisão

com possibilidade de prestação de trabalho até seis meses ou multa. Na mesma linha, a falta de cooperação com a PPC e a obstrução de sua investigação é punível com multa. Estas sanções são adicionadas àquelas já impostas pela PPC pela violação da APPI.

Já no que se refere às decisões do PPC, ao titular é possível que se valha, além de recursos administrativos, de vias judiciais para contestar suas ações e omissões, sendo providenciado pela legislação japonesa vias de recurso administrativo e judicial. Interessante pontuar os casos de omissão da PPC, sendo possível que o titular solicite à PPC a emissão de um ato ou uma orientação administrativa. Ainda, é possível destacar a possibilidade de um titular entrar com ação de indenização estatal contra a PPC em casos de ter ocorrido danos devido à uma ordem ilícita da PPC à um operador comercial ou a PPC não ter exercido sua autoridade em determinado assunto (caso de omissão).

Por fim, a decisão toca nos critérios e regras específicas de acesso a dados por autoridades pública do Japão, com enfoque principalmente em justificativas de interesse público, aplicação do direito penal e de segurança nacional. Como este não é objeto de estudo desta dissertação, este tópico não será por agora explorado.

4.4 Achados parciais

Em relação ao direito doméstico, as decisões de adequação proferidas entre 2000 e 2012 apontam, em sua maioria, apenas para qual o status do direito à privacidade e proteção de dados pessoais (se constitucional ou não), qual a lei de proteção de dados em vigor no país, qual a extensão de sua aplicabilidade. No que toca ao último ponto, este varia entre (i) se a sua aplicação ocorre em relação a todos os setores da economia; (ii) se somente às atividades de tratamento do setor privado ou público e (iii) se somente aos tratamentos automatizados ou qualquer tipo de tratamento de dados pessoais.

De forma genérica, as afirmações da decisão foram no sentido de que os países cumprem com os padrões da Diretiva 95/46/CE e, raras vezes, a decisão apontou para tipos de direitos e princípios garantidos (como o de acesso e exatidão dos dados pessoais) e para regime de tratamento diferenciado em caso de dados sensíveis. Em outras palavras, pouco aprofundamento foi dado às especificidades dos padrões de tratamento dos dados pessoais que de fato vigem no terceiro avaliado. Por exemplo, a Comissão Europeia ressaltou algumas vezes que (i) o regime avaliado está baseado na Diretiva; (ii) a autoridade de proteção possui competência segundo artigo 28 da Diretiva; (iii) o regime de transferência internacional de dados não é mais abrangente do que aquele contido na Diretiva.

Ainda sobre as decisões proferidas entre 2000 e 2012, a avaliação que recaiu sobre à autoridade supervisora tratava de considerações genéricas, apontando quem era a autoridade e que esta gozava de independência, porém não foram destacados os contornos e a forma da independência da supervisão, tendo em sua maioria somente mencionado os poderes de

intervenção e investigação. Em algumas decisões (por exemplo a da Nova Zelândia e Uruguai), a Comissão Europeia ressaltou que a autoridade de controle do país garante os critérios expostos no artigo 28 da Diretiva 95/46/CE, sem, no entanto, se aprofundar em demonstrar a similaridade existente de fato entre as regras implementadas pelo país e aquelas contidas na União Europeia.

Em relação aos compromissos internacionais, destaca-se que países são bem vistos quando aderiram ou são signatários de instrumentos como as Diretrizes da OCDE, Convenção 108, Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais de 1950, do Conselho da Europa, assim como o Pacto Internacional de Direitos Civis e Políticos das Nações Unidas, aprovada em 1996. Trata-se de pontos positivos considerados em relação ao terceiro analisado porque sinalizam seus compromissos com a proteção da privacidade e dos dados pessoais. Não goza desta mesma presunção, todavia, aqueles países membros da APEC Privacy Framework, visto que a Comissão Europeia decidiu que se deve considerar as transferências para estes países como sendo de caráter internacional devido ao regime menos protetivo.

Os Estados Unidos, por sua vez, apesar de ter sido avaliado ainda sob a Diretiva 95/46/CE, destoa das decisões anteriores visto tratar de uma relação em que os termos do tratamento é fruto de um Acordo celebrado entre autoridades da União Europeia e Estados Unidos, estando a decisão de adequação avaliando não o sistema jurídico do país, nem mesmo uma lei específica, mas tão somente as regras e o nível de proteção do Acordo e sua implementação. Este último voltado para uma avaliação quanto ao *enforcement*, fiscalização e remédios judiciais disponíveis aos titulares da UE.

Os Estados Unidos, no entanto, possuem relações antiga com a Comissão Europeia, tendo celebrado no começo dos anos 2000 o Acordo *Safe Harbor*, que foi invalidado no Caso *Schrems vs. Data Protection Commissioner*. Em seguida, negociações levaram ao novo Acordo *Privacy Shield*, esse sob análise da nova decisão de adequação nas relações que se estabelecem entre UE-EUA. É possível apontar que a grande preocupação da UE em relação ao sistema jurídico dos EUA recai em dois eixos centrais (i) a ausência ou a insuficiência de fiscalização do cumprimento das regras pelas empresas autocertificadas e (ii) a vigilância massiva desenvolvida por autoridades de inteligência americana, como apontado, por exemplo, com o programa PRISM.

Por fim, a última decisão proferida foi a do Japão, já sob a vigência do GDPR. Também se trata de uma decisão mais aprofundada do que aquelas proferidas entre 2000-2012. Trata-se de uma decisão que avaliou uma lei específica aplicada aos operadores comerciais e quando os padrões nela contidos fugiam do modelo europeu, a Comissão Europeia estabeleceu normas específicas e complementares a serem cumpridas nas relações Japão-União Europeia ou, ainda, em certas hipóteses, estabeleceu que se aplicassem conceitos definidos no próprio direito da União Europeia (caso de aplicação do conceito de anonimização nos termos definidos no GDPR). Estas exigências recaem, no entanto, somente na medida em que o operador comercial no Japão esteja tratando dados transferidos por outro agente estabelecido na União Europeia -e não

necessariamente aos dados coletados no Japão.

5 CONSIDERAÇÕES FINAIS

Conforme apontado ao longo desta dissertação, a transformação digital e tecnológica potencializou as preocupações dos Estados em proteger a privacidade e os dados pessoais tanto no âmbito de sua jurisdição quanto em relação à transferência destes dados a países terceiros. Esta preocupação extraterritorial se dá muito por conta da facilidade do fluxo dos dados entre fronteiras atualmente, o qual passou a ocorrer de forma célere (quase instantânea) e permitindo uma quantidade massiva de dados. Diante desse contexto, a justificativa de se preocupar com uma lógica pela qual a proteção adequada dos dados os seguem independente do seu lugar de tratamento busca, de todo modo, afastar que outras jurisdições ofereçam (i) sistema menos adequado de proteção, (ii) bem como incentivo para que as atividades de tratamento sejam para lá desviadas, visto que, muitas vezes, a regulação mais protecionista impõe custos adicionais às empresas relacionados à conformidade com a legislação.

No mesmo sentido, outro movimento surgiu relacionado a preocupações de que medidas regulatórias visando a proteção da privacidade e dos dados pessoais pudessem impor restrições ou barreiras ao comércio e transações internacionais. Regulações protecionistas, com regras de armazenamento local ou condições fortes para autorização da transferência podem impor custos altos para o negócio sem necessariamente garantir a segurança e proteção dos dados pessoais almejadas.

O melhor cenário, visto da perspectiva do direito europeu, parece ser aquele em que os países terceiros passem a adotar os seus padrões de proteção, de tal forma que se garante um livre fluxo de dados pessoais que almeja a conformidade global. De que os padrões europeus buscam fortalecer e trazer o indivíduo ao centro do gerenciamento dos dados pessoais disso não se põem dúvidas. Todavia, a forma pela qual a União Europeia vem cobrando a conformidade com seus padrões não parece apontar para um sistema inclusivo ou mesmo aberto às diferentes possibilidades de tratamento de dados que possam ocorrer em diversos sistemas jurídicos e institucionais, voltados às especificidades do país em questão.

Assim, apesar da Comissão Europeia em diversos contextos ter reconhecido que o tema da privacidade e proteção dos dados pessoais é vinculado ao contexto local de sua aplicação e interpretação, as suas exigências em relação às atividades de tratamento e garantia dos direitos dos titulares parecem cada vez mais não se preocupar com fronteiras (visto o fortalecimento da regulação contida na Diretiva para o GDPR). O objetivo parece simples: estas regras e direitos devem ser garantidos desde que os dados em tratamento tenham origem no território europeu. A sua execução, no entanto, demanda esforços e burocracia estatal sofisticada. Para cumprir com isso, a União Europeia busca também formas alternativas à decisão de adequação, como nos casos em que requer que agentes de tratamento de dados se amarrem contratualmente de forma a

garantir o nível de proteção adequado no tratamento de dados pessoais.

Adicionalmente, o fato de que a privacidade e a proteção de dados dependem do fator contextual, social e cultural ao qual o sistema jurídico se insere levanta questionamentos acerca da viabilidade e possibilidade de harmonização global do tema e a eliminação, portanto, das barreiras entre fronteiras. Isto porque mesmo que a União Europeia consiga uma certa uniformidade de padrões de proteção de dados através dos países do globo, a forma de aplicação, interpretação, monitoramento e fiscalização depende do direito na prática, os quais nem sempre são correspondentes (fazendo jus aquela dicotomia entre o *law in books and law in action*) e podem variar de acordo com as autoridades que interpretam e investigam as atividades, bem como com o contexto em que se insere a indústria e os negócios locais.

A possibilidade de organizações internacionais liderarem o tema também não pareceu ter sido até aqui o *locus* de discussão mais frutífero visto que leis de proteção de dados pessoais em geral possuem aplicação tanto para o setor público como privado e se estendem a todos os setores da economia. As organizações internacionais se mostraram especializadas ou foram consideradas *locus* em que o alcance do consenso apresentava obstáculos, diminuindo a capacidade do denominador comum de proteção (visto a transversalidade do tema e os múltiplos interesses envolvidos de diversos setores da economia).

A diversidade no tratamento entre Estados Unidos e União Europeia fez com que mecanismos novos fossem criados para adaptar as exigências do país e do bloco. Assim, por meio de um Acordo que previu a possibilidade de conformidade por meio da autocertificação das empresas, possibilitou-se a criação de um livre fluxo de dados entre EUA-UE restrito ao âmbito das empresas autocertificadas. Conforme já comunicado pela própria Comissão, a conformidade EUA-UE parece apontar uma via interessante para reforçar a conformidade global, visto o poder da aliança no tema entre o país e o bloco.

Contudo, o modelo de autocertificação, conforme exposto, é restrito à relação desenvolvida entre EUA-UE. Pois, nas demais decisões de adequação proferidas pela Comissão Europeia, a avaliação recaia sobre o sistema jurídico do país ou de uma lei aplicada a certos operadores comerciais (caso do Canada e Japão, por exemplo, estando assim abarcados pelo livre fluxo de dados pessoais somente aquelas organizações sujeitas à legislação avaliada pela Comissão Europeia). Nesta última situação, quando a organização sujeita a uma legislação interna considerada adequada pela Comissão Europeia tiver que transferir dados dos titulares da UE para um terceiro localizado em seu próprio país, as regras de transferência internacional de dados voltam a ser aplicadas, visto que o terceiro não está abarcado pela decisão. Cabendo então a uma empresa localizada no Japão, por exemplo, tratar uma transferência a uma organização não abarcada pela APPI (lei de proteção de dados pessoais do Japão) como sendo uma transferência de caráter internacional.

Por fim, podemos concluir que para haver diminuição significativa da restrição do fluxo de dados entre fronteiras é necessário, do ponto de vista europeu, de um certo grau de harmonização

entre legislações domésticas, de forma a garantir a proteção adequada aos direitos, princípios e garantias de proteção de dados pessoais. Todavia, a harmonização que a Comissão Europeia busca por meio da decisão de adequação estaria voltada para uma análise do direito na prática do país, o qual parece pouco provável que esteja espelhado de forma apropriada no processo de avaliação da decisão de adequação.

Referências

AARONSON, S. Why trade agreements are not setting information free: The lost history and reinvigorated debate over cross-border data flows, human rights, and national security. *World Trade Review*, Cambridge University Press, v. 14, n. 4, p. 671–700, 2015. Citado 3 vezes nas páginas 28, 46 e 85.

AGHAEI, S.; NEMATBAKHSH, M. A.; FARSANI, H. K. Evolution of the world wide web: From web 1.0 to web 4.0. *International Journal of Web & Semantic Technology*, Academy & Industry Research Collaboration Center (AIRCC), v. 3, n. 1, p. 1–10, 2012. Citado 2 vezes nas páginas 46 e 47.

ANTONIALLI, D. M. Privacy and international compliance: When differences become an issue. In: *2010 AAAI Spring Symposium Series*. [s.n.], 2010. Disponível em: <https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1165/1470>. Citado na página 51.

BAUER, M. et al. *The costs of data localisation: Friendly fire on economic recovery*. [S.l.], 2014. Nenhuma citação no texto.

BENNETT, C. J. The european general data protection regulation: An instrument for the globalization of privacy standards? *Information Polity*, IOS Press, v. 23, n. 2, p. 239–246, 2018. Citado na página 44.

BERRY, R.; REISMAN, M. Policy challenges of cross-border cloud computing. *J. Int'l Com. & Econ.*, HeinOnline, v. 4, p. 1, 2012. Citado na página 48.

BIONI, B. R. Xeque-mate: o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no brasil. *USP-Grupo de Pesquisa em Políticas Públicas para o Acesso à Informação. Relatório de Pesquisa*, 2016. Citado na página 35.

BIONI, B. R. *Proteção de dados pessoais: a função e os limites do consentimento*. [S.l.]: Forense, 2019. Nenhuma citação no texto.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. lei geral de proteção de dados pessoais - lgpd. *Diario Oficial [da] Republica Federativa do Brasil*, Brasılia, DF, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 20 abr. 2020. Citado na página 20.

BYGRAVE, L. A. Privacy and data protection in an international perspective. *Scandinavian studies in law*, v. 56, n. 8, p. 165–200, 2010. Citado na página 25.

CHEUNG, A. S.; WEBER, R. H. *Privacy and legal issues in cloud computing*. [S.l.]: Edward Elgar Publishing, 2015. Citado 3 vezes nas páginas 49, 50 e 51.

CIURIAK, D.; PTASHKINA, M. The digital transformation and the transformation of international trade. *RTA Exchange. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and the Inter-American Development Bank (IDB*, 2018. Citado 2 vezes nas páginas 21 e 28.

COMISSÃO EUROPEIA. Decisão 2000/518/ec. c(2000)(2304). 2000. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. Decisão 2000/520/ce. 2000. Disponível em: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:PT:HTML>. Acesso em: 20 abr. 2020. Citado 3 vezes nas páginas 78, 88 e 93.

COMISSÃO EUROPEIA. Decisão 2002/2/ec. c(2001) (4359). 2001. Disponível em: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002>. Acesso em: 20 abr. 2020. Citado 2 vezes nas páginas 94 e 102.

COMISSÃO EUROPEIA. Decisão 2003/821/ec. c(2003) (4309). 2003. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0821>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. Decisão 2003/940/ec. c(2003) 490. 2003. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. Decisão 2004/411/ec. c(2004) 1556. 2004. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0411>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. Decisão 2008/393/ec. c(2008) 1746. 2008. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0393>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. Decisão 2010/146/ec. c(2010) 1130. 2010. Disponível em: <https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32010D0146>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. Decisão 2010/635/eu. c(2010) 7084. 2010. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0625>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. Decisão 2011/61/eu. c(2011) 332. 2011. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. ComissÃo europeia. comunicaÇÃo da comissÃo ao parlamento europeu e ao conselho restabelecer a confiança nos fluxos de dados entre eu e os eua. (com(2013) 846 final). 2013. Disponível em: <https://ec.europa.eu/transparency/regdoc/rep/1/2013/PT/1-2013-846-PT-F1-1.Pdf>. Acesso em: 20 abr. 2020. Citado na página 83.

COMISSÃO EUROPEIA. ComunicaÇÃo da comissÃo ao parlamento europeu e ao conselho sobre o funcionamento do sistema «porto seguro» na perspetiva dos cidadãos da ue e das empresas estabelecidas na ue. 2013 (com(2013)847 final). 2013. Disponível em: <https://ec.europa.eu/transparency/regdoc/index.cfm?fuseaction=list&n=10&adv=0&coteId=1&year=&number=847&dateFrom=&dateTo=&serviceId=&documentType=&title=&titleLanguage=&titleSearch=EXACT&sortBy=NUMBER&sortOrder=DESC>. Acesso em: 20 abr. 2020. Citado 2 vezes nas páginas 81 e 82.

COMISSÃO EUROPEIA. Decisão 2013/65/eu. c(2012) 95557. 2013. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013D0065>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

COMISSÃO EUROPEIA. Comunicação da comissão ao parlamento europeu, ao conselho, ao comité económico e social europeu e ao comité das regiões – estratégia para o mercado Único digital na europa (com(2015)192 final). 2015. Disponível em: <https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2015/0192/COM_COM(2015)0192_PT.pdf>. Acesso em: 20 abr. 2020. Citado na página 57.

COMISSÃO EUROPEIA. Decisão 2016/1250/ec. c(2016) (4176). 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG>. Acesso em: 20 abr. 2020. Citado na página 108.

COMISSÃO EUROPEIA. Decisão 2019/419/ec. c(2019) 304. 2019. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC>. Acesso em: 20 abr. 2020. Citado 5 vezes nas páginas 116, 117, 119, 121 e 122.

CORY, N. *Cross-border data flows: Where are the barriers, and what do they cost?* [S.l.], 2017. Disponível em: <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>. Citado 2 vezes nas páginas 28 e 29.

COUNCIL OF EUROPE. Convention for the protection of individuals with regard to automatic processing of personal data. Strasbourg, v. 108, 1981. Disponível em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108>. Acesso em: 20 abr. 2020. Citado 2 vezes nas páginas 33 e 34.

CUNNINGHAM, M. Complying with international data protection law. *U. Cin. L. Rev.*, HeinOnline, v. 84, p. 421, 2016. Citado 5 vezes nas páginas 44, 75, 76, 77 e 78.

DONEDA, D. *Da privacidade à proteção de dados pessoais*. [S.l.]: Renovar Rio de Janeiro, 2019. Citado 2 vezes nas páginas 24 e 25.

DRAKE, W. J. Background paper for the workshop on data localization and barriers to transborder data flows. In: *The World Economic Forum*. [S.l.: s.n.], 2016. p. 14–15. Nenhuma citação no texto.

EETEN, M. J. V.; MUELLER, M. Where is the governance in internet governance? *New media & society*, Sage Publications Sage UK: London, England, v. 15, n. 5, p. 720–736, 2013. Nenhuma citação no texto.

FERRACANE, M. Restrictions on cross-border data flows: a taxonomy. ECIPE Working Paper, 2017. Citado 5 vezes nas páginas 27, 28, 29, 30 e 31.

GIURGIU, L.; BARSAN, G. The prosumer–core and consequence of the web 2.0 era. *Journal of Social Informatics*, v. 9, n. 1, p. 53–59, 2008. Citado na página 47.

GOLDSMITH, J. L. Against cyberanarchy. *The University of Chicago Law Review*, JSTOR, v. 65, n. 4, p. 1199–1250, 1998. Disponível em: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1001&context=occasional_papers>. Nenhuma citação no texto.

GREENLEAF, G. Global data privacy laws: Forty years of acceleration. *Privacy Laws and Business International Report*, n. 112, p. 11–17, 2011. Citado na página 15.

GREENLEAF, G. Global data privacy laws: 89 countries, and accelerating. *privacy laws & business international report*, n. 115, 2012. Citado na página 15.

GREENLEAF, G. The influence of european data privacy standards outside europe: implications for globalization of convention 108. *International Data Privacy Law*, Oxford University Press, v. 2, n. 2, p. 68–92, 2012. Citado na página 15.

GREENLEAF, G. Global data privacy laws 2015: 109 countries, with european laws now a minority. *Privacy Laws Business International Report*, 2015. Citado na página 19.

GREENLEAF, G. 'european'data privacy standards implemented in laws outside europe. *Data Privacy Standards Implemented in Laws Outside Europe (September 3, 2017)*, v. 149, p. 21–23, 2017. Citado na página 15.

GREENLEAF, G. Global convergence of data privacy standards and laws: Speaking notes for the european commission events on the launch of the general data protection regulation (gdpr) in brussels & new delhi, 25 may 2018. *UNSW Law Research Paper*, n. 18-56, 2018. Citado na página 15.

GREENLEAF, G. Global data privacy laws 2019: 132 national laws & many bills. *Privacy Laws Business International Report*, p. X, 2019. Citado na página 19.

ICO. Adtech market research report. *INFORMATION COMMISSIONER'S OFFICE*, 2019. Disponível em: <https://ico.org.uk/media/about-the-ico/documents/2614568/ico-ofcom-adtech-research-20190320.pdf>. Acesso em: 20 abr. 2020. Citado na página 55.

ICO. Update report into adtech and real time bidding. *INFORMATION COMMISSIONER'S OFFICE*, 2019b. Disponível em: <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>. Acesso em: 20 abr. 2020. Citado 2 vezes nas páginas 52 e 55.

JOHNSON, D. R.; POST, D. Law and borders: The rise of law in cyberspace. *stanford law review*, JSTOR, p. 1367–1402, 1996. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=535>. Nenhuma citação no texto.

KUNER, C. An international legal framework for data protection: Issues and prospects. *Computer law & security review*, Elsevier, v. 25, n. 4, p. 307–317, 2009. Citado 5 vezes nas páginas 10, 38, 39, 40 e 42.

KUNER, C. Regulation of transborder data flows under data protection and privacy law: past, present, and future. *TILT Law & Technology Working Paper*, n. 016, 2011. Nenhuma citação no texto.

KUNER, C. Reality and illusion in eu data transfer regulation post schrems. *German Law Journal*, Cambridge University Press, v. 18, n. 4, p. 881–918, 2017. Nenhuma citação no texto.

LANGER, M. From legal transplants to legal translations: The globalization of plea bargaining and the americanization thesis in criminal procedure. *Harv. Int'l LJ*, HeinOnline, v. 45, p. 1, 2004. Nenhuma citação no texto.

LEONARDI, M. Internet: Elementos fundamentais in responsabilidade civil na internet e nos demais meios de comunicação. *São Paulo: Saraiva*, 2012. Citado 2 vezes nas páginas 47 e 48.

MANYIKA, J. et al. *Digital globalization: The new era of global flows*. [S.l.]: McKinsey Global Institute San Francisco, 2016. v. 4. Citado 2 vezes nas páginas 21 e 22.

MELL, P.; GRANCE, T. et al. The nist definition of cloud computing. Computer Security Division, Information Technology Laboratory, National . . . , 2011. Citado na página 48.

MOEREL, L. *Binding corporate rules: corporate self-regulation of global data transfers*. [S.l.]: OUP Oxford, 2012. Citado na página 74.

MOSCO, V. *Becoming digital: Toward a post-internet society*. [S.l.]: Emerald Group Publishing, 2017. Nenhuma citação no texto.

NASSER, S. H. *Fontes e normas do direito internacional: um estudo sobre a soft law*. [S.l.]: Editora Atlas, 2006. v. 2. Nenhuma citação no texto.

NEWMAN, A. *Protectors of privacy: Regulating personal data in the global economy*. [S.l.]: Cornell University Press, 2008. Nenhuma citação no texto.

NEWMAN, J. M. Antitrust in zero-price markets: Foundations. *University of Pennsylvania Law Review*, JSTOR, p. 149–206, 2015. Nenhuma citação no texto.

OECD. *OECD guidelines on the protection of privacy and transborder flows of personal data*. [S.l.]: OECD Publishing, 2002. Nenhuma citação no texto.

OECD. *The evolving privacy landscape: 30 years after the OECD privacy guidelines*. [S.l.]: OECD Publishing, 2011. Citado 3 vezes nas páginas 32, 33 e 35.

OECD. *Cloud Computing: The Concept, Impacts and the Role of Government Policy*. OECD Publishing, Paris, 2014. Disponível em: <http://dx.doi.org/10.1787/5jxzf4lcc7f5-en>. Citado 3 vezes nas páginas 49, 50 e 52.

PARLAMENTO EUROPEU. Diretiva 95/46/ce do parlamento europeu e do conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. *Jornal Oficial da União Europeia*, Bruxelas, 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 20 abr. 2020. Citado 4 vezes nas páginas 43, 68, 70 e 71.

PARLAMENTO EUROPEU. Directiva 2009/136/ce do parlamento europeu e do conselho de 25 de novembro de 2009 que altera a directiva 2002/22/ce relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas, a directiva 2002/58/ce relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas e o regulamento (ce) n.o 2006/2004 relativo à cooperação entre as autoridades nacionais responsáveis pela aplicação da legislação de defesa do consumidor. *Jornal Oficial da União Europeia*, Bruxelas, 2009. Disponível em: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:PT:PDF>. Acesso em: 20 abr. 2020. Citado na página 53.

PICKER, R. C. Completion and privacy in web 2.0 and the cloud. *Nw. L. Rev. Colloquy*, HeinOnline, v. 103, p. 1, 2008. Citado 3 vezes nas páginas 48, 49 e 51.

QUEIROZ, R. M. R. Direito à privacidade e proteção aos dados pessoais: aproximações e distinções. *Revista do Advogado*, n. 144, 2019. Citado na página 24.

SCHWAB, K. *A quarta revolução industrial*. [S.l.]: Edipro, 2016. Citado 2 vezes nas páginas 22 e 23.

SELBY, J. Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both? *International Journal of Law and Information Technology*, Oxford University Press, v. 25, n. 3, p. 213–232, 2017. Citado 3 vezes nas páginas 29, 30 e 31.

SHAFFER, G. Globalization and social protection: the impact of eu and international rules in the ratcheting up of us privacy standards. *Yale J. Int'l L.*, HeinOnline, v. 25, p. 1, 2000. Nenhuma citação no texto.

SOLUM, L. B.; CHUNG, M. The layers principle: Internet achitecture and the law. *Notre Dame L. Rev.*, HeinOnline, v. 79, p. 815, 2003. Citado na página 46.

SOLUM, L. B.; CHUNG, M. The layers principle: Internet achitecture and the law. *Notre Dame L. Rev.*, HeinOnline, v. 79, p. 815, 2004. Nenhuma citação no texto.

TFUE. Caso schrems v. data protection commissioner (case c-362/14). *Tribunal de Justiça da União Europeia*, 2012. Disponível em: <https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF>. Acesso em: 20 abr. 2020. Citado na página 85.

TJUE. Caso schrems v. data protection commissioner (case c-362/14). *Tribunal de Justiça da União Europeia*, 2015. Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362>. Acesso em: 20 abr. 2020. Citado 5 vezes nas páginas 84, 85, 86, 87 e 89.

UNIÃO EUROPEIA. Carta dos direitos fundamentais da união europeia. *Jornal Oficial da União Europeia*, Bruxelas, 2000. Disponível em: <https://www.europarl.europa.eu/charter/pdf/text_pt.pdfAcessoem20.04.2020>. Acesso em: 20 abr. 2020. Citado 3 vezes nas páginas 16, 23 e 86.

UNIÃO EUROPEIA. Regulamento nº 679, de 27 de abril de 2016. general data protection regulation. *Jornal Oficial da União Europeia*, Bruxelas, 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679>. Acesso em: 20 abr. 2020. Citado 2 vezes nas páginas 20 e 21.

VOIGT, P.; BUSSCHE, A. Von dem. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, Springer, 2017. Citado na página 58.

WALDMAN, A. E. Privacy as trust: Sharing personal information in a networked world. *University of Miami Law Review*, HeinOnline, v. 69, p. 559, 2015. Citado 3 vezes nas páginas 25, 26 e 27.

WALDMAN, A. E. *Privacy as trust: information privacy for an information age*. [S.l.]: Cambridge University Press, 2018. Citado na página 26.

WARREN, S. D.; BRANDEIS, L. D. The right to privacy. *Harvard law review*, JSTOR, p. 193–220, 1890. Citado 2 vezes nas páginas 24 e 25.

WORKING PARTY. Article 29 – data protection working party. opinion 3/2000 on the eu/us fialogue concerning the "safe harbor" arrangement (wp31). 1999. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp31_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 77.

WORKING PARTY. Article 29 – data protection working party. opinion 4/2000 on the level of protection provided by the "safe harbor principles" (wp32). 1999. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 77.

WORKING PARTY. Article 29 – data protection working party opinion 7/99 on the level of data protection provided by the "safe harbor" principles as published together with the frequently asked questions (faqs) and other related documents on 15 and 16 novermber 1999 by the us department of commerce (wp 27). 1999. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp27_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 77.

WORKING PARTY. Article 29 – data protection working party. working document on the current state of play of the ongoing discussions between the european commission and the united states government concerning the "international safe harbor principles". 1999. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp23_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 77.

WORKING PARTY. Article 29 – data protection working party. opinion 1/99 concerning the level of data protection in the united states and the ongoing discussions between the european commission and the united states government. 1999a. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp15_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 77.

WORKING PARTY. Article 29 – data protection working party. opinion 2/99 on the "adequacy of the international safe harbor principles" issued by the us department of commerce on 19 april 1999. 1999b. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp19_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 77.

WORKING PARTY. Article 29 – data protection working party. opinion 4/99 on the frequently asked questions to be issued by the us department of commerce in relation to the proposed "safe harbor principles". 1999c. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp21_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 77.

WORKING PARTY. Article 29 – data protection working party. working document: Transfers of personal data to third countries: Applying article 26 (2) of the eu data protection directive to binding corporate rules for international data transfers. 2003. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 61.

WORKING PARTY. Article 29 – data protection working party. working document on a common interpretation of article 26 (1) of directive 95/46/ec of 24 october 1995. 2005. Disponível em: <https://ec.europa.eu/newsroom/article29/news-overview.cfm>. Acesso em: 20 abr. 2020. Nenhuma citação no texto.

WORKING PARTY. Article 29 – data protection working party. opinion 2/2010 on online behavioral advertising (wp 171). 2010. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 54.

WORKING PARTY. Article 29 – data protection working party. opinion 16/2011 on easa/iab best practice recommendation on online behavioural advertising (wp188). 2011. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp188_en.pdf>. Acesso em: 20 abr. 2020. Citado na página 54.

WORKING PARTY. Article 29 – data protection working party. opinion 04/2012 on cookie consent exemption (wp 194). 2012. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdfAcessoem7.04.2020>. Acesso em: 20 abr. 2020. Citado na página 54.

WORKING PARTY. Article 29 – data protection working party. guidelines on automated individual decision-making and profiling for the purposes of regulation 2016/679 (wp251rev.01). 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>. Acesso em: 20 abr. 2020. Citado na página 56.